Security Threats in Remote Workforce Environment

Semester project report for Network/Internet Security, Dr. Dipankar Dasgupta instructing

Ramita Maharjan, U000769429
Department of Computer Science, University of Memphis, Memphis, TN, rmhrjan1@memphis.edu

ABSTRACT

Thanks to the development of the internet and technology, people today can work from anywhere. While remote working is not new, its popularity has never been on such a massive scale as it became in 2020. This sudden ascent in the number of teleworkers and businesses that allow teleworking is because of the worldwide spread of Coronavirus. With the rise in teleworking, the risks of cyber-attacks are very high due to the nature of home networks. People in the same household often share devices, accounts, and networks for personal and professional works which could endanger the sensitive information of everyone in the family and even the organizational confidential data could be exposed and disclosed. Therefore, both the organization and remote workers should take necessary steps to prevent malicious attacks, identify and resolve such cyber incidents and revise and strengthen the incident response plan to prevent sensitive data and information from future attacks.

1 Introduction

The Covid-19 global pandemic caused a sudden shift from the physical workplace to the virtual workplace in many businesses that they were not prepared for. Distance work arrangements allow employees to work virtually from any corner of the world. Teleworking is new to many people but the sudden shift to remote working has started becoming the new normal. According to Owl Labs report, almost 70% of full-time workers in the U.S are working from home during COVID-19, and 1 in 2 people will not return to jobs that do not offer remote work [1]. Global Workplace Analytics launched a “Global Work-from-Home Experience Survey” and it estimates that about 25% to 30% of the workforce will be working remotely from home by the end of 2021 [2] .

Home networks are inherently less secure than the corporate network as they lack network security solutions such as firewalls, secure gateways, network mappers, port scanners, and packet analyzers which enhance the security. This pandemic-induced transition to remote working has given an unprecedented and humongous number of opportunities for cybercriminals and malicious users, thus making the security arrangements of the remote workforce a critical priority to the organizations. According to NIST, a cyber threat is any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service. Trend Micro reports that there were over 1.2 million attempts made to compromise remote login services, with 89% of these attacks being executed through brute force [3]. The 2020 Cyber Threatscape report from Accenture Cyber Threat Intelligence reveals that there has been a

60% increase in the average ransom payment (US$178,254) from the first quarter to the second quarter of 2020 [4]. Some of the common cybersecurity threats that employees and businesses working remotely are phishing attacks, DDoS attacks, spam emails, malicious domains/websites, malware, ransomware, malicious social engineering, and many more. In this study, we are going to address the security challenges from the employees' point of view as well as employers' point of view and suggest preventive measures that help minimize the risks of cybersecurity threats in remote working.

2 Objectives of the Study

The main objectives of this study are the followings:

i. To identify the security risks remote work has on businesses and employees.
ii. To suggest measures to mitigate the risks associated with remote work.
iii. To suggest ways to empower employees to securely telework.

3 Literature Review

In April 2020, United States' Cybersecurity and Infrastructure Security Agency (CISA) and UK's National Cyber Security Center (NCSC) released a joint alert providing on exploitation by a cybercriminal and advanced persistent threat (APT) groups of the current coronavirus disease 2019 (COVID-19) global pandemic [5]. It contains a summary of threats observed such as phishing, malware distribution, credential theft, and the exploitation of new teleworking infrastructure. CISA has been continuously providing and updating alerts about different ransomware activities and suggesting tips to combat those risks.

In Nov 2020, McAfee published its second quarterly threat report and observed an average of 419 threats per minute. McAfee's global network of more than a billion sensors registered a 605% increase in total Q2 COVID-19-themed threat detections. New office malware spiked 103% and new PowerShell malware increased 117% [6].

In Feb 2021, Palo Alto Networks detected attempts to exploit vulnerabilities in firewalls, VPNs, switches, and routers. The report says that the goal of the attacks is to plant malware in the devices and join them in a botnet to distribute more malware. On Feb. 23, 2021, one of the IPs involved in the attack was updated to serve a Mirai variant leveraging CVE-2021-27561 and CVE-2021-27562, mere hours after vulnerability details were published. On March 3, 2021, the same samples were served from a third IP address, with the addition of an exploit leveraging CVE-2021-22502. Furthermore, on March 13, an exploit targeting CVE-2020-26919 was also incorporated into the samples [7].

In March 2021, the FBI (Internet Crime Complaint Center (IC3)) released a 2020 internet crime report including Covid-19 scam statistics. The complaints surged to 791,790 in 2020, representing a 69.4% rise over 2019 and the total losses involved exceeded $4.2 billion. Phishing scams, non-payment/non-delivery scams, and extortion were the three most reported crimes. The IC3 received over 28,500 complaints related to COVID-19, with fraudsters targeting both businesses and individuals [8].

A huge number of researchers are working to identify various risks involved with teleworking, safety measures, and improve remote working security. Mandal and Khan have discussed security threats in the cloud as a passive impact of the Covid-19 pandemic in remote learning, working from home, and in healthcare, banking, and e-commerce industries in [9]. They have also listed some preventive measures that can help stop spreading cyber threats. In another paper [10], the authors Khan, Brohi, and Zaman have explained about the top 10 cybersecurity threats amid the Covid-19 pandemic which includes DDoS attacks, malicious domains and websites, malware, spam emails, and so on. They have also discussed about the organizations and industries that are mostly at the risk of cyber-attacks given the world situation.

4 Cybersecurity Threats

There are different ways a malicious attacker may attempt to harm or illegally access sensitive business and personal data for their personal benefits and financial gain. Given below are some of the cybersecurity threats that are mostly used to breach a remote workforce environment by the cybercriminals:

- **Phishing:** Attackers may use legitimate-looking telework software, websites, or phishing links to gain sensitive information. According to an IC3 report, phishing scams proliferated in 2020, more than doubling from 114,702 in 2019 to 241,342 in 2020 [8]. Treasury Department's Financial Crimes Enforcement Network (FinCEN) says that tens of thousands of new website domains have been registered with terms related to COVID-19 and the response to it, such as “quarantine”, “vaccine” and “CDC” since Jan 2020.

- **Spam emails:** Business email compromise scams exploit both personal and professional emails by compromising personal emails, vendor emails, spoofing lawyer email accounts, requesting W-2 information, etc. As fraudsters have been exploiting the fear of the Coronavirus, people are receiving a huge number of spam emails related to contact tracing, Covid testing, Covid-cases update/alerts, stimulus payments, vaccines, phony remedies, and so on.

- **Eavesdropping:** Malicious actors are targeting communication tools such as video conferencing software, VOIP phones, and cloud-based communication systems to eavesdrop on business conversations and private meetings. In March 2020, Zoom reached more than 200 million daily meeting participants [11]. Several people have faced zoom bombing and video-teleconferencing hijacking attempts that insert pornographic images, hate images, or threatening language during the conversations.

- **DDoS attacks:** Attackers can launch DDoS attacks and render businesses and e-commerce sites unavailable for financial gain, hacktivism, cyber warfare, and revenge.

- **Malware:** The McAfee Q2 report (2020) indicated malware being the top disclosed attack vector accounting for 35% of publicly reported incidents and the total malware exceeded 1.2 billion. This is followed by account hijacking, targeted attacks, unknown attacks, malicious attack vectors, and so on [6].

- **Ransomware:** On March 17, 2021, CISA release an alert about “TrickBot” malware, an advanced Trojan that malicious actors spread by spearphishing campaigns using tailored emails [12]. On March 23, 2021, IC3 released a flash alert about Mamba ransomware that weaponizes DiskCryptor and has been deployed against different services and businesses [13]. Some of the top ransomware attacks of 2020-2021 are Revil, Sodinokibi, Nemty, Nephilim, NetWalker, DoppelPaymer, Ryuk, and so on.
- **Malicious Social Engineering:** The use of remote work applications such as Zoom, WebEx, Google Meet, and others used for virtual meetings and screen sharing have extensively surged, and with this comes the malicious opportunities for social engineering, as invites for these applications can be spoofed for phishing attempts.
- **Identity Theft:** Identity theft happens when someone steals personal information to commit fraud. In 2020, FTC reported 1.387,615 cases of identity theft which is double the number a year earlier. The victims of the identity theft cases said that their information was used to apply for or receive government benefits such as unemployment compensation. The identity thief may use the fraudulently acquired person’s private identifying information to apply for credit, file taxes, or get medical services.

5 Security Issues in Remote Working

The confidential and sensitive information of businesses has always been a target for cybercriminals. The malicious actors are always trying to launch cyberattacks in different forms for this purpose and businesses need to pay very special attention to the security of their data and devices. Now, the maintenance of security measures and the protection of its digital data and information has been more challenging due to the added risks from a remote working environment. Typically, attackers tend to take advantage of the following security issues in remote working that the telecommuters often tend to overlook.

Shared Devices: Remote working is much riskier because there will be several network appliances connected to the home network such as laptops, mobiles, desktops, tablets, televisions, Internet of Things such as smart home devices, security systems, wearables, and many more. It is very common for people living together to share such devices with each other. Even if the employee has been provided with a company-issued device, employees using work-issued devices for personal reasons or any person using such device is a cybersecurity nightmare. Slight negligence and unhygienic behavior while using the device for freelancing and side jobs, emails, attachment downloads, browsing and shopping online, logging to social networking sites or other accounts, saving passwords and personal files, using for financial transactions can put the employee himself, all his family members and even the organization at huge risk.

Shared Accounts: Shared accounts are any resource that uses a single pair of credentials to authenticate multiple users. People living under the same roof often share accounts. For instance, in most cases, only a single member in a house subscribes to accounts such as Netflix and is shared among all the members. The shared credentials may be re-shared. People tend to use the same password for multiple accounts or similar passwords. They may even be using single sign-on such as signing using google or Facebook on multiple platforms. Therefore, the person who was given one set of credentials to be able to access multiple systems that they may not have been granted access to. This can ease up the hackers to guess the passwords or even get direct access to the shared account. All the sensitive information such as health/medical records, travel plans, financial information are at high risk of being exposed.

Shared network: The majority of home networks use a common network where several network devices including personal, home, and professional devices are connected wirelessly or by network cables. A single router is used as a gateway to the outer network. The security of all the devices is at high risk if any one of the devices or accounts is compromised. It is not only the sensitive personal information of the individuals at home that is at risk but also the organization's confidential data is subject to breach and unauthorized access.

A malicious actor tries to break into a home network due to its inherent vulnerabilities. The attacker may be using viruses, trojans, spyware, ransomware, phishing, man-in-the-middle attacks, and other threats to obtain sensitive information, be it personal or business-related. The cybersecurity risks are much more in-home networks because multiple people have full access to machines sharing different accounts and a network.

6 Mitigation Measures for the Risks

The National Institute of Standards and Technology (NIST) has provided guidelines on telework and remote access to help organizations mitigate security risks associated with the enterprise technologies used for teleworking, such as remote access servers, telework client devices, and remote access communications. In 2016, NIST issued a guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security which is still relevant today [18]. The United States Secret Service Cybercrime Investigations has published a guide for preparing for a cyber incident which is classified into how to understand, prepare, execute, and debrief a cyberattack [16]. In 2015, the Department of Justice published "Best Practices for Victim Response and Reporting of Cyber Incidents" and which was revised in 2018 [19]. Based on the guidelines and suggestions from these three sources, the following mitigation measures are identified for the cybersecurity threats in remote working:

A. Before the attack: Preventive measures

Organization:

i. **Security awareness training:** In a remote work setting, the responsibility of maintaining cyber-secure hygienic behavior lies on all the teleworkers and other employees who may work in hybrid and physical workplaces. So, organizations should conduct proper cybersecurity training and provide information about the exploitations cyber actors can attempt, using secured VPN connections for accessing enterprise data and resources, securing, and updating end devices such as routers, firewall, personal devices, using strong passwords, avoiding shared networks, devices, and accounts and where and how to report and seek help from in case of attacks.

ii. **Telework Security policy:** A telework security policy should have tiered levels of remote access with each level providing a set of rights and permission to access organization data. This helps in controling the access to organizations' data and it should also include the policies for accessing remote servers and updating those servers. A telework security policy should define which forms of remote access the organization permits, which types of telework devices are permitted to use each form of remote access, and the type of access each type of teleworker is granted.

iii. **Multi-factor authentication:** There’s always a possibility that malicious actors will attempt to gain illegal access to the organizational data and resources, telework client devices, and leverage those devices to access enterprise networks. Organizations must secure the data stored on client devices by encrypting all the sensitive data. For enterprise access, multi-factor authentication is very essential since it can filter out unauthorized access and even discourage shared accounts. Multi-factor authentication strengthens user accounts by adding an extra layer of authentication such as OTP, push notification, or biometrics (all forms of biometrics cannot be used in remote work setting).

iv. **Encryption technology:** Organizations must be aware that communications on networks outside of the organization’s control are susceptible to eavesdropping, interception, and modification. Although, using encryption technologies as well as authenticating each of the endpoints to each other to verify their identities helps mitigate such dangers, there’s not 100% guarantee. VPN is the most common approach for tunneling that uses cryptography to protect the confidentiality and integrity of communications. It is also better to be proactive and encrypt data before storing.

v. **Secure servers:** The remote access servers must be secured effectively because they are responsible for providing a secured, isolated telework environment for organization-issued, third-party-controlled, and BYOD client devices. A server should be located within an organization’s network perimeter so that it acts as a single point of entry to the network and enforces the telework security policy. The servers, other devices, and routers must be up-to-date and secured by changing all default passwords to strong passwords, updating with the latest security patches after appropriate testing, discontinuing the use of vulnerable devices that have not been patched by the vendor, and disabling Universal Plug and Play (UPnP) on routers unless it is necessary for business operations.

vi. **Secure telework client devices:** All the client devices such as desktops, laptops, smartphones, and tablets must also be secured against common threats including malware, device loss or theft, and social engineering. Local security controls such as applying operating system and application updates promptly, disabling unneeded services, and using anti-malware software and a personal firewall must be implemented. For better security of sensitive data, encryption techniques are highly recommended for data stored on the devices.

vii. **Network traffic monitoring and threat analysis:** Apart from maintaining the security of the server, client devices, communication channels, it is very important to monitor the network traffic for threat prevention and analysis. Such tools can ensure that the network services are online, available, and operating to the full capacity by avoiding performance issues, tracking bandwidth usage, and highlighting suspicious activity. As detailed in IBM's Cost of a Data Breach Report 2020, companies on average take 207 days to identify a data breach and another 73 days to contain the attack. A lot of damage can be done before a cyberattack is recognized and contained.

viii. **Regular backup of files:** Access to confidential information is the goal of every cyberattack because by leveraging such information the attackers can have their demands or ill-wish fulfilled. Therefore, encrypting the information and storing it in an encrypted file storage device should be done regularly by businesses [16].

Teleworkers:

i. **Cybersecure behavior:** Despite the high level of security infrastructures maintained by the enterprise, small negligence of the remote home workers can jeopardize the integrity, confidentiality, and availability of the enterprise data and resources. Therefore, teleworkers must be extra vigilant before clicking on links, evaluate the web browser's security settings before providing sensitive information or downloading anything, and locking the device when not in use, using strong passwords. CISA has published "Telework reference materials for the at-home worker" which includes a lot of tips on avoiding social engineering and phishing attacks, safeguarding the data, understanding firewalls, protecting against ransomware, and much more [14].

ii. **Secure home network:** Many home users have a misconception that their home network is too small to be at the risk of a cyberattack but with teleworkers accessing organizational data, the risk has now grown more than ever. While the work-issued devices are secured by the organization, there are many personal devices and IoT devices which require regular software updates, removing unnecessary services and software, adjusting factory-default configurations. The teleworkers can use antivirus, install network and device firewalls, disable Wi-Fi protected setup (WPS) and turn the network off when not in use [15].

iii. **Network slicing:** The home networks should be partitioned so that work-issued devices and personal devices are operated on a separate network. This can be done by using the concept of network slicing which requires the addition of a couple of routers. As a result, the gateway router in the home network can separate traffic into two routers: one for work devices and another for personal devices. Network slicing employs isolation of traffic and bandwidth among multiple slices in addition to providing independent control and the ability to customize and modify a slice to optimize the application according to specific needs.

iv. **User partitioning:** A logical partitioning of users can be done so that multiple users can access the same hardware and system resources but cannot encroach on other users' resources. User partitioning can minimize the risks of sensitive information being exposed if any other users in the home network has his/her account compromised.

B. During the attack:

i. **Assess the incident:** Informing the IT department (Cybersecurity Response Team) is the first step since they can guide through the steps to be followed. Whether the attack was caused by a malicious act, human error, a technological glitch or a combination of these determines the type of assistance needed to mitigate the specific damage. The power should not be switched off if the organization has appropriate logging capabilities because a system administrator may attempt to identify the affected computer systems, the apparent origin of the incident, any malware used, and any remote servers where the data was transferred.

ii. **Document the response:** The protective measures outlined in the Incident Response plan should be implemented to prevent further escalation of the attack. The response should be well documented that include recording the description, dates and times of all incident-related events, technical information of systems, accounts, services, and so on, amount and type of damage inflicted, and many more.

iii. **Preserve evidence:** A remote worker may click pictures of the threats. All the evidence should be preserved which may include server logs, network maps, a list of affected servers, disk images, memory images, copies of malware and ransomware, etc.

iv. **Contact law enforcement and financial entities:** If the incident is caused by malicious attacks, it is crucial to inform law enforcement and they will be providing information on which entities should be contacted further. Financial entities need to be contacted in case of potential financial implications or risks. Remote workers may immediately change passwords for all the online accounts if any of their accounts are compromised.

C. After the attack:

i. **Report the incident**: Based on the type of cybersecurity attack, the incident must be reported to the concerned department.

   i. File a complaint with the FBI at Internet Crime Complaint Center IC3 by visiting https://www.ic3.gov/.

   ii. Report the incidents, phishing, malware, or vulnerabilities to https://us-cert.cisa.gov/report.

   iii. Report incidents such as hacking and password trafficking, internet fraud, and spam to U.S. Secret Service on https://www.secretservice.gov/contact/field-offices.

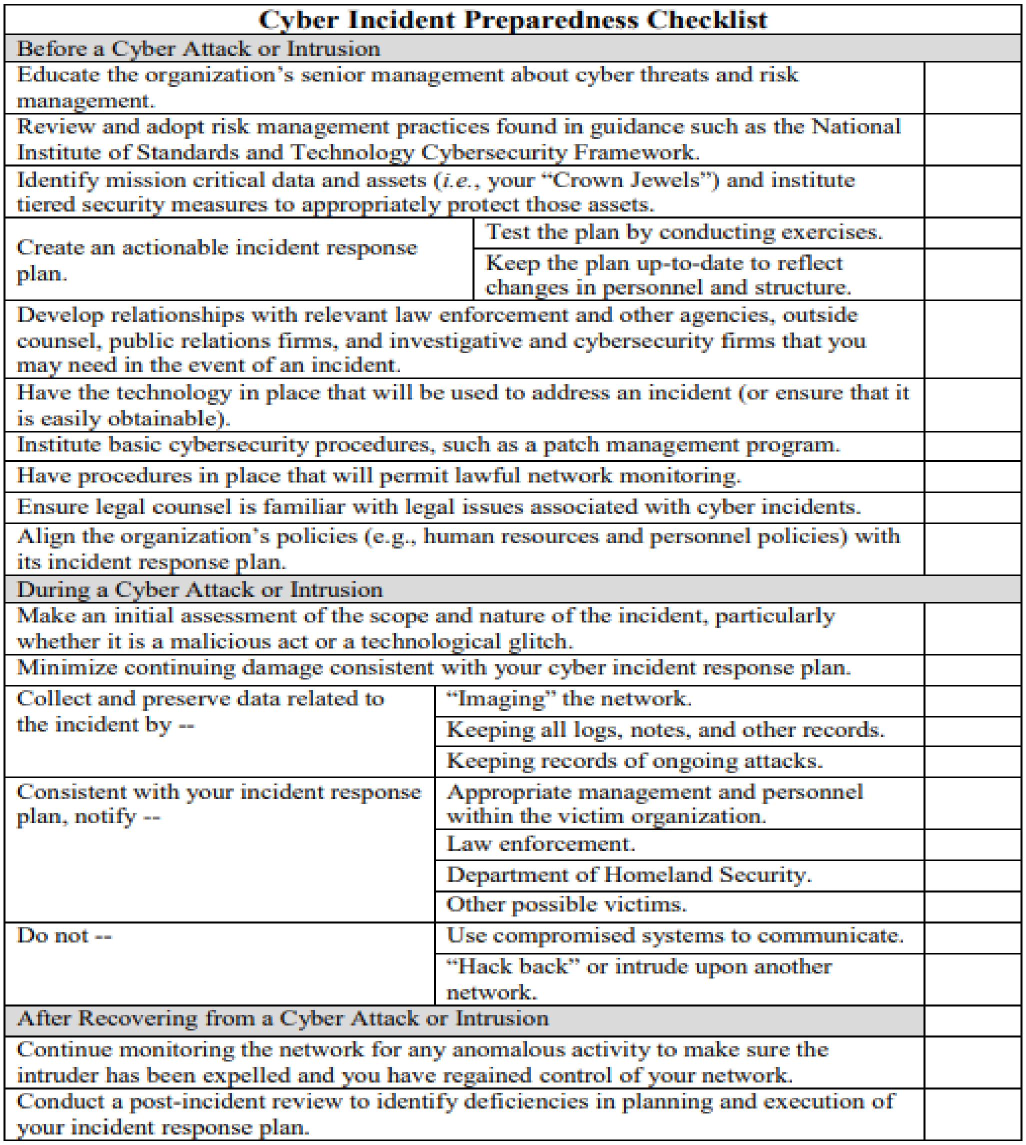
   iv. File a report with the Office of the Inspector General (OIG) in case of Social Security number misuse on https://www.identitytheft.gov/ or call the Social Security Administration hotline at 1-800-269-0271 [17].

   v. Report incidents relating to national security and infrastructure issues to the Department of Homeland Security's National Infrastructure Coordinating Center at 202-282-9201.

ii. **Continue monitoring**: The network and systems monitoring should be continued to ensure that the cyber incident is under control and for further potential malicious activities. The affected system may be re-infected and compromised which requires proper vigilance of the system.

iii. **Conduct post-incident review and adjust the Response Plan**: After the cyberattack is resolved, a review should be conducted to find out the deficiencies, shortcomings, and gaps in the system, network, and Cyberattack Response plan. Necessary steps must be taken to overcome the effects of the weaknesses reported and adjust the plan accordingly to prevent the damage of similar attacks in the future.

"Best Practices for Victim Response and Reporting of Cyber Incidents" provided by Department of Justice sums up how businesses could assess their preparedness against a cyber incident in the form of the following cyber incident preparedness checklist.



Cyber Incident Preparedness Checklist		
Before a Cyber Attack or Intrusion		
Educate the organization's senior management about cyber threats and risk management.		
Review and adopt risk management practices found in guidance such as the National Institute of Standards and Technology Cybersecurity Framework.		
Identify mission critical data and assets (*i.e.*, your "Crown Jewels") and institute tiered security measures to appropriately protect those assets.		
Create an actionable incident response plan.	Test the plan by conducting exercises.	
	Keep the plan up-to-date to reflect changes in personnel and structure.	
Develop relationships with relevant law enforcement and other agencies, outside counsel, public relations firms, and investigative and cybersecurity firms that you may need in the event of an incident.		
Have the technology in place that will be used to address an incident (or ensure that it is easily obtainable).		
Institute basic cybersecurity procedures, such as a patch management program.		
Have procedures in place that will permit lawful network monitoring.		
Ensure legal counsel is familiar with legal issues associated with cyber incidents.		
Align the organization's policies (e.g., human resources and personnel policies) with its incident response plan.		
During a Cyber Attack or Intrusion		
Make an initial assessment of the scope and nature of the incident, particularly whether it is a malicious act or a technological glitch.		
Minimize continuing damage consistent with your cyber incident response plan.		
Collect and preserve data related to the incident by --	"Imaging" the network.	
	Keeping all logs, notes, and other records.	
	Keeping records of ongoing attacks.	
Consistent with your incident response plan, notify --	Appropriate management and personnel within the victim organization.	
	Law enforcement.	
	Department of Homeland Security.	
	Other possible victims.	
Do not --	Use compromised systems to communicate.	
	"Hack back" or intrude upon another network.	
After Recovering from a Cyber Attack or Intrusion		
Continue monitoring the network for any anomalous activity to make sure the intruder has been expelled and you have regained control of your network.		
Conduct a post-incident review to identify deficiencies in planning and execution of your incident response plan.		

Figure 1: Cyber Incident Preparedness Checklist [19]

7 Software Tools for Remote Working

The security of remote working is a broad topic and it depends on how secured every single software/tool used in the teleworking is because a small loophole or vulnerability in any software being used puts the whole organization at huge risk. Day-to-day communication and meetings is a vital part of remote work for which Zoom is the most popular platform and it allows end-to end encryption with Advanced Encryption Standard (AES) 256. Zoom also has other features such as creating waiting rooms, expel/suspent a participant, audio signatures and many more to keep the communication more secured [20]. However, there are many vulnerabilities found in Zoom such as "CWE-200: Exposure of Sensitive Information to an Unauthorized Actor" published on March 18, 2021 by NIST [21]. Many other tools such as Microsoft Teams, Webex, GoToMeeting, Skype, Messenger etc. also have end-to-end encryption.

In addition, it is important to access remote telework devices or organization machines using tools such as TeamViewer which secures its traffic using RSA and AES(256-bit) session encryption[22]. RemotePC is another tool which uses TLS v 102/AES-256 encryption for securing data transfers between local and remote computers during remote sessions [23]. Similarly, there are a lot of solutions for endpoint security software such as ESET Endpoint Security, Avast Business, LogMeIn Central, CrashPlan and many more. A VPN can prevent unnecessary insecurities and tools like PureVPN, Norton Secure VPN, GOOSE VPN, Pangeo are some of the Virtual Private Network software that can be used in remote working. Likewise, Duo Security, LastPass, Okta, JumpCloud are some of the authentication software for multifactor authentication.

With so many options available in the market for collaboration, communication, security, productivity and project management for working remotely, the security of teleworking depends largely on using the right software tools. It is the responsibility of every organization to look into security features available in different products and choose the best one for enhancing the security of remote work environment against external threats and attacks.

8 Conclusion

With the huge influx of employees in the remote work setting, cybercriminals are active now more than ever. Businesses have been spending a significant portion of their budget on cybersecurity and protecting the organization's data and devices from outside attacks. Because of remote data access from multiple devices and so many applications being hosted in the cloud, the traditional cybersecurity perimeter no longer exists. Some seemingly usual workers' behavior such as sharing devices, accounts, and home networks could be a door for launching cyberthreats. The unauthorized access to business information can jeopardize sensitive personal information and vice versa. It is as much as the duty of an employee to protect the critical business data as it is the responsibility of the organization. Therefore, both the teleworkers and businesses need to take necessary precautions to prevent cyber incidents and appropriate responses and actions during and after such attacks if such incidents happen.

References:

1. https://resources.owllabs.com/state-of-remote-work/2020

2. https://globalworkplaceanalytics.com/work-at-home-after-covid-19-our-forecast
3. https://www.trendmicro.com/vinfo/us/security/research-and-analysis/threat-reports/roundup/securing-the-pandemic-disrupted-workplacetrend-micro-2020-midyear-cybersecurity-report
4. https://www.accenture.com/_acnmedia/PDF-137/Accenture-2020-Cyber-Threatscape-Executive-Summary.pdf
5. https://us-cert.cisa.gov/ncas/alerts/aa20-099a
6. https://www.mcafee.com/enterprise/en-us/lp/threats-reports/nov-2020.html
7. https://unit42.paloaltonetworks.com/mirai-variant-iot-vulnerabilities/
8. https://www.fbi.gov/news/pressrel/press-releases/fbi-releases-the-internet-crime-complaint-center-2020-internet-crime-report-including-covid-19-scam-statistics
9. https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9215374
10. Khan, Navid Ali; Brohi, Sarfraz Nawaz; Zaman, Noor (2020): Ten Deadly Cyber Security Threats Amid COVID- 19 Pandemic. TechRxiv. Preprint. https://doi.org/10.36227/techrxiv.12278792.v1
11. https://blog.zoom.us/a-message-to-our-users/
12. https://us-cert.cisa.gov/ncas/alerts/aa21-076a
13. https://www.ic3.gov/Media/News/2021/210323.pdf
14. https://www.cisa.gov/telework-reference-materials-home-worker
15. https://us-cert.cisa.gov/ncas/tips/ST15-002
16. Preparing for a Cyber Incident - An Introductory Guide v 1.1.pdf (secretservice.gov)
17. https://www.identitytheft.gov/
18. https://csrc.nist.gov/CSRC/media/Publications/Shared/documents/itl-bulletin/itlbul2020-03.pdf
19. https://www.justice.gov/criminal-ccips/file/1096971/download
20. Security | Zoom Trust Center
21. NVD - CVE-2021-28133 (nist.gov)
22. TeamViewer Security and Privacy
23. Frequently Asked Questions - RemotePC™ - Security

APPENDIX

Abbreviations

BYOD	Bring your own device
NIST	National Institute of Standards and Technology
WPS	Wi-Fi Protected Setup
FTC	Federal Trade Commission
CISA	Cybersecurity and Infrastructure Security Agency
IC3	Internet Crime Complaint Center

FBI	Federal Bureau of Investigation
NCSC	National Cyber Security Center
APT	Advanced Persistent Threat
DDoS	Distributed Denial of Service
OIG	Office of the Inspector General
OTP	One-time password
VPN	Virtual Private Network
FinCEN	Financial Crimes Enforcement Network