International Journal in IT & Engineering (IJITE)
Volume 8 Issue 6, June 2020 ISSN: 2321-1776 Impact Factor: 6.493
Journal Homepage: http://ijmr.net.in, Email: irjmss@gmail.com
Double-Blind Peer Reviewed Refereed Open Access International Journal

UNDERSTANDING CYBERSECURITY CHALLENGES OF TELECOMMUTING AND VIDEO CONFERENCING APPLICATIONS IN THE COVID-19 PANDEMIC

Kenneth Okereafor, PhD
Deputy General Manager - Database Security,
Department of Information and Communications Technology,
National Health Insurance Scheme (NHIS) Abuja, NIGERIA.
nitelken@yahoo.com

Phil Manny
Founder & Director – Agora Nexus
Director West Africa – Alliance Media Group.
phil.manny@agoranexus.com / phil@alliances.global

ABSTRACT

As a result of restrictions in mass gathering and imposition of social distancing to curtail the spread of COVID-19, there is an unprecedented adoption of telecommuting and video conferencing as innovative technological alternatives for remote work and office administration, colloquially referred to as teleworking, mobile working, home working or "work from home (WFH)". The combination of telecommuting and video conferencing comes with the benefits of reduced overhead, increased productivity and minimal risks of exposure to infectious diseases including the COVID-19 which is spread through human clusters. Unfortunately, the popularity of telecommuting and video conferencing applications has also opened up potential avenues for cyber-attacks and other hostile hacking incidents that target porous networks and unsafe systems and applications, thereby raising serious ethical, cyber security and privacy concerns. This paper examines a comprehensive overview of cyber security issues related to telecommuting and video conferencing applications including their vulnerabilities, threats, and impacts.

Keywords: *COVID-19, cyber-attack, cybercrime, cyber security, remote work, telecommuting, teleworking, WFH.*

1.0 INTRODUCTION

Having spread to all corners of the globe, the infectious coronavirus disease (COVID-19) has influenced a global restriction on social congregation of all types including the traditional workplace. With this reality, millions of businesses have been forced to contend with the option of managing a completely remote workforce with the aid of telecommuting and related technologies. COVID-19 and the mass shift to WFH has provided a digital rocket and a huge cultural shift operationally for every organization across the global. Many technology vendors have already adjusted relevant portions of their product and service offerings to reflect the booming global adoption of WFH. Similarly, organizations across all sectors are implementing remote work policies for their employees, in accordance with this trend.

Technology giants Microsoft, Facebook, Amazon, Twitter, Google, and many others have updated guidelines for their employees to work remotely and balance productivity. At the same time, they are focusing attention on fine-tuning potential connectivity flaws previously existing on their products and services.

The cyber security risks arising from inherent vulnerabilities in remote technologies are not particularly new, but as the social distancing policies of the pandemic compel employees to work more from home and as people seek new ways to stay connected, malicious hackers around the world are also taking advantage of the widespread changes in the workforce attitude and the increase in online activities, to launch large-scale phishing attacks, phone scams and other computer-based exploits against these vulnerabilities. Successful cyber-attacks lead to data loss, reputation damage and technology apathy; and potentially undermine the efforts to contain the spread of COVID-19. In this paper, the first of two series, we examine issues arising from working from home including cyber security risk factors, technological apathies, and impacts of cyber-attacks.

The rest of the paper is structured as follows: **Section 2** discusses the basic components of telecommuting and video conferencing applications. **Section 3** examines the challenges of remote work and reviews their cyber security implications. **Section 4** focuses on the business and technical impacts of WFH-based cyber-attacks. **Section 5** concludes the paper with summary remarks.

2.0 COMPONENTS OF TELECOMMUTING AND VIDEO CONFERENCING

Telecommuting – also called teleworking – is the technology-assisted practice of working remotely or from home by the combined use of internet-connected communication systems, email facilities, the telephone, and other online digital applications. It is the application of computer software and high-speed telecommunication systems to implement workplace-related communications remotely. The video conferencing component is a variation of remote real-time video interaction where participants cluster in a fixed location as opposed to individual participation in traditional teleworking. However, an innovative integration of a video conferencing session as a representative of singular teleworking participant is possible where the segmentation of large participants from different geographic locations is required. Video conferencing solutions can be used for two-way live communication with limited possibilities of interaction with the audiences. Application areas include virtual meetings, online training, technical support, webinar sessions, business conferences, chats rooms, messaging and file sharing, as well as multiparty internet telephony communications.

The current wave of telecommuting has been triggered by the demands of the COVID-19 pandemic and can therefore be referred to as episodic or situational as it is not a scheduled type of routine telecommuting, but one that has been necessitated by an emergency situation. As a result, each vital component of telecommuting presents a unique security challenge [1] that must either be mitigated or closely monitored to minimize the chances of its

circumvention by malicious hackers and internet fraudsters. The components of telecommuting are reviewed below.

2.1 High Speed Data Networks

Fast networks provide the channel through which remote communication links are established and maintained throughout a telecommuting session. They provide the platform for good connectivity required for the systems to retain good quality audio, video, text, and image. Anything that affects the quality and easy accessibility of the data network, could impact on the output, and could potentially diminish the system's integrity and cyber security rating. Available connectivity options include fiber, radio, Wi-Fi connections, mobile networks, etc. The ability of the network component to maintain the confidentiality, integrity and availability of data being transmitted across the session, provides a fair assessment of the overall security of the service, and is usually a basic for technological evaluation.

2.2 Cloud Services

Cloud services are essential for hosting the platform for telecommuting to strive. Cloud services [2] are virtual computing resources (data storage and computing power), made available to users by cloud computing providers on demand via the internet without direct active management by the user. While it is attractive to take advantages of cloud computing, the security aspects in a cloud-based computing environment remain at the core of interest [3] [4].

For the purpose of supporting the remote work, cloud services include the application software, visual presentation utility, web-based plug-ins, dedicated web portals, instant messaging, voice over internet protocol (VOIP), and other complementing programmers. E.g. shared documents programmers such as file storage and synchronization services – Google Drive and Microsoft One Drive, web-based document management application – Google Docs, and file hosting service – Drop Box, all operate under the cloud software as a service (SaaS) model.

2.3 Terminals

Terminals are the end-user connecting devices through which communications and exchange are initiated, received, or controlled from in both telecommuting and video conferencing applications. They include smartphones, laptops, tablets, desktop computers, alongside their peripherals: webcams, monitors, speakers, earpieces, styluses, etc. The functionality of these terminals at any point in time during an established session contributes to the security status and to how safe the transmitted data eventually becomes.

2.4 Security and Protective Utilities

There is a huge list of protective systems that all together add up to provide protection at various stages of a telecommuting session. In addition to protecting the terminals and complementing the cloud services, they also ensure the safety of the medium through interoperability with systems from multiple vendors. Security tools also provide encryption of on-going communications to prevent or minimize the risk of eavesdropping on confidential

information. They also provide quality of service balancing, monitoring and alert mechanisms. E.g. endpoint protections, as well as utility protocols such as virtual private network (VPN) and voice over internet protocol (VoIP).

2.5 Telecommuting Applications

Many telecommuting applications exist from multiple vendors in various forms, serving audiences from diverse backgrounds. Zoom, Cisco WebEx, Slack, Citrix, Skype, and Microsoft Team are among the numerous telecommuting Apps available today. Although the underlying concept remains the same across all applications, the technology implementations and specific features defer from vendor to vendor. E.g. Zoom's *waiting room* feature performs similar functions as Microsoft Team's *lobby*, providing a temporary screening facility to allow the meeting organizer to carry out due diligence on each potential participant prior to granting admittance.

3.0 CHALLENGES OF TELECOMMUTING AND VIDEO CONFERENCING

Challenges are viewed from three broad but interwoven perspectives, namely technological apathies, cybersecurity risk factors and philosophy of cyberattacks on WFH platforms.

3.1 Technological apathies and cultural issues

3.1.1 Employee perspective of technology

From an employee standpoint, there are so many areas of challenge to consider including: the role of the individual in the organization, the assigned level of access to company assets, the operational competence and psychological balance to work alone, IT security awareness, the convenience of the remote environment, as well as technology reliability.

As most organizations transition from traditional architecture to cloud and internet based, many are compelling their staff to sign WFH policy documents as a code of conduct. However, with the increase in phishing emails of over 300% since lockdown, the long-term psychological stress associated with such compulsion needs to be addressed, especially as activity surveillance and productivity monitoring are becoming a norm. In general, the overall WFH cultural changes encompass the technological apathies.

3.1.2 Geography related apathies

The technology reliability in the specific geographic location of the remote workers is an important challenging factor in examining convenience in the shift to WFH, cloud and internet-based architecture. E.g. remote workers in some technologically advanced parts of the world have routine access to reliable 4G (soon to be 5G) unlimited mobile data as well as up to 62MB fibre to the home (FTTH) internet service. These incentives make accessing, downloading, or completing any cloud and internet-based work very easy, as opposed to less developed regions of the world where there are issues of power supply, bandwidth, and access to quality internet services.

3.1.3 Convenience of the working environment

A very important aspect of consideration for the remote worker is the working environment. Many do not have the luxury of a dedicated home office or workspace away from distraction from kids, visitors, and domestic chores. Furthermore, chances of data errors exist from environmental distractions as people working from home get easily distracted by combining work with domestic endeavors including laundry, personal emailing, private web browsing, etc.

For most people, going to the office physically is a sanctuary which entails a 100% focus on the job. Therefore, in looking at the remote environment, the psycho-emotional effects of being isolated and not experiencing the pleasure of seeing and interacting with colleagues deserves serious consideration.

3.1.4 Attitudinal adjustment conflict

Those who have been regularly working from a home office prior to the pandemic as an integral part of work flexibility, and already conversant with using telecommuting applications for remote connections and client interactions around the globe, are most likely to adjust faster to the current COVID-19 induced WFH shift than others. For such people, the current shift is less of a change. However, those whom it is new to are more likely to experience a transitory period of adjustment during which initial resistance and conflict are expected, in addition to some level of isolation and loneliness.

3.2 Cyber security Risk Factors

A number of direct and indirect factors account for the cyber security incidents on WFH systems, and they present burning issues which organizations have to contend with while employees work from outside of a traditional office environment. By design, remote communication systems such as telecommuting and video conferencing applications are bandwidth intensive. This means that they rely heavily on the quantity and quality of connectivity to sustain communications sessions. It also means that anything that affects the stability or quality of the connectivity among the participants could degrade the outcome or lead to total failure, respectively.

Despite their numerous benefits, telecommuting and video conferencing systems have inherent vulnerabilities which cybercriminals and internet spammers take advantage off to perpetrate attacks.

3.2.1 Insecure networks

Poor network conditions and inadequate bandwidth are two major network-related issues with remote video technology. Up to the early 2000s, the legacy internet telephony systems were characterized by high latency, jitters, and echoes on Sipura, Media ring, Delta3, Net2phone and other early VOIP platforms [5]. With progressive research by the Internet Engineering Task Force (IETF), the Institute of Electrical and Electronic Engineers (IEEE) and vendor markets, contemporary solutions have surmounted these initial hiccups.

An unsafe network, especially one comprising of an unregulated, unprotected, or unencrypted channel is a major weakness which can be taken advantage of by malicious hackers to launch cyber-attacks and diminish the quality of the session or disrupt the session entirely. The porosity of an insecure network is easily spotted by the malicious hacker during pre-attack vulnerability scanning while searching for exploitable loopholes. Loopholes in an insecure network can include unencrypted channels, factory default device access credentials, weak authentication protocols, outdated devices drivers, unpatched software, and obsolete operating systems.

3.2.2 Capacity gap with ignorant employees

Ignorance of basic cybersecurity requirements for online engagement particularly for remote collaboration is an indication of corporate capacity gap. An ignorant employee constitutes a major risk to the security of telecommuting as a remote work tool. E.g. early signs of ignorance begin to manifest when virtual meeting notices and login ID for a teleworking session are announced on social networks, making it difficult to monitor and verify the identity of potential participants.

3.2.3 Data security ethical issues

The inability of corporate organizations, employees, and participants in a teleworking session to adhere to online etiquettes regarding sharable information on open networks can become a serious privacy concern that challenges the safety and confidentiality of sensitive data. This also includes how individuals are able to manage their connecting terminals before, during and after each telecommuting session.

3.2.4 Unsafe terminals

An unsafe terminal is one with an underlying security issue or having a poorly protected operating condition capable of affecting the confidentiality, integrity, or availability of the data it processes or of the system it is meant to support. The presence and use of an insecure terminal in a telecommuting session particularly one running on obsolete software or housing an unpatched utility poses a danger to the safe operation of the session. Such insecure terminal presents loopholes which cybercriminals are able to exploit to attack the remote work session either by introducing a disruptive bug or by intercepting the transmitted data and listening in on confidential communication, both of which could potentially result in privacy invasion.

3.2.5 Insider collusion

One of the corporate threats very difficult to manage, and one that is very rampant among organizations, is the conspiracy of direct involvement of an employee in initiating, aiding, or facilitating a cybercrime by deliberately providing an intruder access to a yet-to-be-mitigated loophole on the system. Collusion in telecommuting occurs when two or more legitimate participating employees release meeting IDs or other connection credentials to non-members for malicious intent, or when identified errors are deliberately overlooked to the advantage of the intruder.

3.2.6 Social engineering

Teleworking platforms are very vulnerable to social engineering attacks due to the weaknesses in humans which are mostly taken advantage of by cybercriminals. Social engineering methods use psychological tricks to create deception [6], which in turn makes people to perform actions that could divulge personal and corporate confidential information [7] rather innocently. It is a psychological exploitation which scammers use to skillfully manipulate humans and carry out emotional attacks on innocent people [8], such as on telecommuting and video conferencing platforms.

On a WFH session, a scammer assumes a name that matches a legitimate participant's identity and gains access to the session where he can remain passive throughout the episode. The ability of the attacker to remain passive and extract confidential information constantly from the session compromises the confidentiality of the entire system. In an extreme case, the attacker may choose to become active by disrupting the session through posting of derogatory comments and offensive images which may lead to an outright discontinuation of the session. Such disruptions have ethical and reputational connotations, and could be very scandalous.

3.2.7 Distraction errors

The distraction of mixing WFH and domestic affairs increases the risks that the remote worker can inadvertently introduce malware links into the company's computer network thereby exposing employers and colleagues to various degrees of cyber-attacks, where over 90% of which are delivered by email related services. Many remote workers are likely to fall victim to distraction errors including wrong entries and delayed responses, given the currently disrupted management communications occasioned by the COVID-19 lockdown.

3.3 Cyber-attacks on WFH platforms

3.3.1 Man-in-the-middle attack

In the man-in-the-middle (MiM) attack, the attacker, using special hacking tools, intercepts a telecommuting communication channel and eavesdrops on on-going conversation. The purpose of this attack can be passive or active. A passive man-in-the-middle attack simply intercepts the conversation, and records or merely listen in without disruption. Such passive attacks only have impact on the data confidentiality as the attacker can capture confidential picture, record secret data or access sensitive documents being transmitted along the communications channel. An active MiM attack on the other hand seizes data between two nodes [9], causes actual disruption and modification [10] or alters part of the intercepted data such that its content, quality, and integrity are compromised. Advanced forms of MiM attack can also completely delete data from the channel, or cause delayed delivery of data exchanged over the virtual meeting session.

MiM attack is possible on any unencrypted or poorly secured cloud based remote work application, whether WebEx, Zoom, Microsoft Team, or others. The concept of zoom bombing is a MiM attack specifically targeted at gaining unauthorized access, wherein the

adversary inserts his clandestine identity into the session, and listen in, gathers corporate sensitive information that can potentially be used for espionage or other cybercrimes.

Vulnerability in the zoon app is the potential for people to take advantage of the publicly announced session logon and join the meeting and in the middle of the conversation begin to post inappropriate content or use other forms of offensive attack such as cyber bullying to disrupt the session.

3.3.2 DDoS attack

With a distributed denial of service (DDoS), the attacker's target is to disrupt the entire teleconferencing session by deliberately overloading the system with so much unnecessary traffic that it overwhelms its capacity to cope, thereby leading to a malfunction, a breakdown or incessant bouts of reboots. A DDoS impacts negatively on system performance and can potentially lead to participants' frustration.

4.0 IMPACTS OF CYBERATTACKS ON WFH APPLICATIONS

The consequences of successful breaches and cyber-attacks [1] on WFH applications could have an overbearing impact on work quality and turnaround time but could also impose privacy implications.

4.1 Identity theft

Sensitive data being transmitted across unsafe telecommunication channels and poorly protected telecommuting terminals can be intercepted by internet fraudsters and used for fraudulent bank transactions, gain unauthorized assess, activate ransom advantage, or be simply modified for use in future cyber criminalities. Depending on the nature and sensitivity of the stolen corporate data, loss of trade secrets can threaten the survivability of the organization. In the healthcare sector, loss or unauthorized modification of patient's medical records can lead to misdiagnosis and fatalities both which have long term reputational consequences.

4.2 Privacy issues

Data leaks are rampant among insecure telecommuting systems due to poor access control mechanisms to detect, prevent of proactively respond to cyber security breaches. The resulting privacy breaches have a long-term negative effect on the reputation of the organization and could trigger costly litigations, operational disruption, or overall ripple effect on operational sustenance.

4.3 Accessibility issues

With slow networks, remote working could become a nightmare affecting the prompt availability of data at the point of need. Delayed access to data could impose life-threatening impacts on organizations that rely on the timeliness of data access for services such as banking transactions, emergency healthcare, aviation control, and crime forensics.

5.0 CONCLUSION

Work from home (WFH) provides an opportunity to sustain corporate productivity when physical gathering is risky or prohibited such as the COVID-19 pandemic. WFH would be impossible without the fantastic telecommuting technologies available today as an enabler of mobility, allowing colleagues to communicate and collaborate in real-time from different geographic locations. At the same time, the gains of working from home tend to be contending with the risks of exposure to cyber threats and malicious hackers who capitalize on unsafe networks and insecure systems to circumvent the remote communication experience. This paper has examined the cyber security, ethical and technological loopholes in remote working. It also identified their impacts on the employer's data as well as the employee's online safety.

The second paper, and concluding part of this two-part series titled *"Solving the Cyber security Challenges of Telecommuting and Videoconferencing Applications in the COVID-19 Pandemic"*, proposes cyber security mitigation actions that can be applied both now and in the post COVID-19 era to make WFH, virtual meetings, webinars, and teleconferences safer alternatives to direct communications in times of mobility restrictions.

Caveat

The conclusions and views expressed in this paper are the authors' personal opinions, and do not necessarily represent the opinions of any organization(s) to which they are affiliated. Names of specific vendors, manufacturers, products, services, or institutions wherever mentioned or implied in this paper are for illustrative, educational, and informational purposes only. Implicit or expressed mention of such names of specific vendors, manufacturers, products, services, or institutions does not suggest authors' preference, endorsement or recommendation of the vendors, manufacturers, products, services, or institutions so mentioned. Similarly, non-mention of specific vendors, manufacturers, products, services, or institutions does not suggest authors' disapproval or apathy against such vendors, manufacturers, products, services, or institutions.

ABOUT THE AUTHORS

Kenneth Okereafor is a United Nations trained Cyber security expert, and Deputy General Manager at the National Health Insurance Scheme (NHIS) Nigeria, where he oversees Database Security and Health Informatics. With a PhD in Cyber security & Biometrics from Azteca University Mexico, he has accumulated over two decades of professional ICT experience, and has acquired special skills in applying Cyber Threat Intelligence & Mitigation Technologies to detect, prevent and respond to Cyberattacks in industry,

government, and academia. Kenneth is a member of the International Organization for Standardization's Technical Committee on Health Informatics (ISO-TC-215), and he currently chairs ISO's Security and Privacy Working Group-4 in Nigeria, developing and adopting Cybersecurity standards for Nigeria's digital health ecosystem. He has research interests in, and publications on, Global Cybersecurity Operations, Incident Response, Multi-biometrics, Electronic Health Security, Computer Forensics, and Digital Identities; and may be reached at nitelken@yahoo.com.

Phil Manny is the Founder & Director of Agora Nexus (www.agoranexus.com), and Regional Director, West Africa of Alliance Media Group (www.alliances.global). He is an Economics graduate of Cardiff University UK, Business School, and has spent the last 12 years running B2B C-level events and programmes across the globe with a focus on Sub-Saharan Africa. With experience across multiple sectors including O&G, IT, Power, and Shipping, Phil prides himself on understanding and learning of cultural and regional diversity in business.

REFERENCES

[1] K. Okereafor and R. Djehaiche, "A Review of Application Challenges of Digital Forensics," *International Journal of Simulation Systems Science and Technology*, vol. 21, no. 2, pp. 35.1 - 35.7, 2020.

[2] Sally Adam, "Coronavirus and remote working: what you need to know," Sophos, 12 March 2020. [Online]. Available: https://news.sophos.com/en-us/2020/03/12/coronavirus-and-remote-working-what-you-need-to-know/?id=0013000001JH0eX. [Accessed 31 May 2020].

[3] M. Ahmed and M. A. Hossain, "CLOUD COMPUTING AND SECURITY ISSUES IN THE CLOUD," *International Journal of Network Security & Its Applications (IJNSA)*, vol. 6, no. 1, pp. 25-36, 2014.

[4] Hibatullah Alzahrani, "A Brief Survey of Cloud Computing," *Global Journal of Computer Science and Technology: B Cloud and Distributed*, vol. 16, no. 3, pp. 10-16, 2016.

[5] Y. Fayyaz, D. M. KHAN and F. FAYYAZ, "The Evaluation of Voice-over Internet Protocol (VoIP) by means of Trixbox," *International Journal of Natural and*

Engineering Sciences, vol. 10, no. 3, pp. 33-41, 2016.

[6] K. Okereafor and O. Adebola, "Tackling the Cybersecurity Impacts of the Coronavirus Outbreak as a Challenge to Internet Safety," *International Journal in IT and Engineering (IJITE)*, vol. 8, no. 2, pp. 1-14, 2020.

[7] M. Choudhary, A. Kumar and N. Kumar, "Social Engineering in Social Networking Sites: A Survey," *International Journal of Engineering Research & Management Technology (IJERMT)*, vol. 3, no. 1, pp. 123 - 129, 2016.

[8] B. Atkins and W. Huang, "A study of social engineering in online frauds," *Open Journal of Social Sciences*, vol. 1, no. 3, p. 23, 2013.

[9] B. Celiktas and M. S. TOK, "MAN IN THE MIDDLE (MITM) ATTACK DETECTION TOOL DESIGN," *INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY*, vol. 7, no. 8, pp. 90-99, 2018.

[10] G. Hao and G. Tao, "Principle of and Protection of Man-in-the-middle Attack Based on ARP Spoofing," *Journal of Information Processing Systems*, vol. 5, no. 3, pp. 131-134, 2009.

[11] John Emmitt, "Top 10 Cybersecurity Threats in 2020," Kaseya Company, 15 April 2020. [Online]. Available: https://www.kaseya.com/blog/2020/04/15/top-10-cybersecurity-threats-in-2020/. [Accessed 21 May 2020].

[12] Eoin Carroll, "Transitioning to a Mass Remote Workforce – We Must Verify Before Trusting," McAfee, 7 April 2020. [Online]. Available: https://www.mcafee.com/blogs/other-blogs/mcafee-labs/transitioning-to-a-mass-remote-workforce-we-must-verify-before-trusting/. [Accessed 17 May 2020].