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

SOLVING 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

In the wake of the global lockdown necessitated by the COVID-19 pandemic, the adoption of telecommuting and remote video technologies to support real-time remote audio-visual communications has become widespread. The mass adoption of virtual office communication techniques using various work from home (WFH) implementations has become very beneficial in facilitating real-time business conversations, saving revenue and time, as well as containing the spread of COVID-19. Despite its numerous benefits as a reliable substitute for direct human-to-human close proximity communications, the technology also faces threats and vulnerabilities which malicious hackers have capitalized on to insert offensive content, obstruct conversations and intercept confidential information. The challenges have been identified alongside their impacts on privacy and security. This paper proposes cybersecurity mitigation actions that can secure WFH platforms, telecommuting and video conferencing applications, and make them safer alternatives to direct communications both now and potentially in the post COVID-19 era.

Keywords: *COVID-19, cyberattack, cybersecurity, remote work, telecommuting, threat, video conferencing, vulnerability, WFH.*

1.0 INTRODUCTION

COVID-19 and the mass shift to WFH has provided a huge cultural and operational shift for every organization across the global. A pandemic lockdown of this magnitude has never happened in the modern era with organizations being thrown in at the deep end with continuous learnings on a daily basis.

As social distancing policies have compelled a huge proportion of employees to work from home, and as people seek new ways to stay connected, the patronage of remote work platforms has risen exponentially; but the main concern for any company operating with

remote workers is IT security, where each company has a different level of vulnerabilities, exposures, security requirements, and response strategies.

The first part of this paper titled *"Understanding the Cybersecurity Challenges of Telecommuting and Videoconferencing Applications in the COVID-19 Pandemic"* had presented an overview of cybersecurity issues related to telecommuting and videoconferencing technologies including a comprehensive examination of their vulnerabilities, threats, and impacts. This paper, the second in the two-part series, proposes preventive and detective countermeasures for mitigating cybersecurity challenges found in remote communications systems, for a safer experience.

The rest of the paper is structured as follows: **Section 2** discusses the basis for cybersecurity intervention in WFH implementations. **Section 3** proposes remedies for tackling the identified challenges including preventive and detective controls required for securing remote work assets from cyberattacks. **Section 4** concludes the paper with summary remarks.

2.0 THE NEED FOR CYBERSECURITY SOLUTION

Security is a key concern in all remote work platforms, especially as the need for WFH continues to rise in accordance with the COVID-19 lockdown requirements, bringing more application areas to the fore. Telecommuting and video conferencing applications have found more frequent use at this time for transmitting audio and video interactions of work-related participants across different locations who are engaged in real-time communications using high-speed telecommunications system. Application areas include:

- Meeting – online meeting, training, technical support
- Webinar – sales, product promotion, marketing events, town hall sessions
- Conference rooms – collaborations, business discussions, partnerships
- Telephony – Multiparty phone system
- Chat – messaging and file sharing across platforms
- Remote learning – accessing academic classes and tutorials online
- Virtual research – sharing research outputs remotely among researchers

The security expectations of employees when they work remotely are convenience, privacy, and safe computing, and they want to see these expressed in the quality of protection of company data transmitted across networks as well as the safe management of sensitive documents shared among legitimate participants. Maintaining the confidentiality, integrity, and availability of data over remote work platforms is the ultimate desire of every organization adopting remote work [1] implementations, even as the protection of people's physical health is held in high esteem. Hence the threat to cybersecurity health is not relegated to the background.

3.0 MITIGATION COUNTERMEASURES

In addition to having a properly setup home office comprising of the right work environment, suitable desks, chairs, monitors, Wi-Fi and other required hardware, the following cybersecurity mitigations are imperative to guarantee reasonable protection in the cyberspace.

3.1 Preventive controls

Preventive controls are precautionary in nature and are therefore expected to have been in place already, or existing in an on-going basis.

3.1.1 Proper setup

Although there are factory default settings, it is a good security practice to meticulously check for the correctness of the configurations of the systems used for remote work applications. Ensuring that the systems are properly setup, and that the configurations are suitably secured is a sure way to establishing a safe posture.

3.1.2 Updated and fully patched system

The underlying operating systems of all computers designated for use in WFH and telecommuting should be properly updated and possibly running the most current version of the operating systems and utilities. A smart way to achieve this is by automating the management of system updates and patches for effective protection against potential cyber threats. This practice prevents cyberattacks that take advantage of vulnerabilities existing in obsolete programmes and services. In addition to operating systems, all software application layers [2], antivirus software, VPNs and telecommuting applications should be properly updated and promptly patched as applicable.

3.1.3 Full featured cloud services

Where cloud services e.g. Google Drive's file storage and synchronization, Microsoft's OneDrive, or any other software-as-a-service (SaaS) offering is required as an integral part of telecommuting and remote work, it is a more secure practice to purchase the full commercial version rather than the free edition that may come with limited protection and encryption, of which the end user license agreement (EULA) could impose traffic [3] monitoring and surveillance.

3.1.4 Virtual meeting links

Meeting participation IDs or attendance links should not be posted on public forum such as a social media platforms and blogs because they could be highjacked and used for zoom bombing, espionage, and service disruption. Meeting invitation links are best communicated individually.

3.1.5 Secure meeting ID

The automated meeting ID generated upon setup of a remote conference is a product of an algorithm that is completely predictable and vulnerable, therefore a strong password is required to secure the meeting ID to control who actually logs in and participates at the meeting. In addition to a passworded ID, the use of descriptive IDs should be avoided. Using

non-obvious meeting ID increases the attacker's burden of guess and minimizes the chances that targeted cyberattacks can ever be successful.

3.1.6 Controlled session

There are two telecommuting and video conferencing functionalities that should be used during each session to minimize zoom bombing. The first is the *waiting room* feature that allows all meeting members to go through a transitory waiting area before they are allowed to join the actual meeting, giving the meeting moderator the opportunity to track and verify authorized participants, or possibly take a roll call.

The second is the *lock the meeting* features which is used to lock the meeting after all participants have joined. The lock functionality restricts further entry and so that no new participants can join even if they have the meeting ID and password. This helps to reduce the chances of adversaries sneaking in undetected to spy, eavesdrop or steal data.

These two, and more features, should be applied to consolidate security and trust in telecommuting applications. The illustrative terms *waiting room* and *lock the meeting* are terminologies adopted by a specific remote communications product, but other products have various terms for referring to their own versions of similar features.

3.2 Detective controls

Detective controls provide visibility into malicious activities on the WFH or other remote work implementations, including event logs associated with monitoring the network and alerting the user.

3.2.1 Antivirus and endpoint security

As attacks are purely unpredictable, it is a good security practice to configure the security settings of antivirus solutions, associated devices, systems, and threat detection software properly to defend against exploitable loopholes. Deploying advanced solutions that provide endpoint detection and response (EDR) is a sure way to keep systems proactively secure.

3.2.2 Wireless encryption

A poorly configured wireless access point (AP) becomes attractive to the adversary and there are many targeted attacks on APs. It is imperative to enable full encryption [4], full authentication, and to set strong passwords [3]. Once this is done on the device, it is secure and locked down, and the device compromise is potentially prevented.

3.2.3 Password management

Since passwords are the most widely used authentication means, their formulation and use in remote work systems and terminals should conform with global standards particularly specifications by the National Institute of Standards and Technology (NIST) and the SANS Institute [5] [6] [7], for strength, complexity and usability. All security ethics involving

password reuse across personal and work systems, and other similar practices should be strictly adhered to.

3.2.4 Multi factor authentication

Oftentimes passwords are too easy to guess and too hard to remember, and this creates a password chaos for the user to keep track, resulting in unsafe password fatigue habits including choosing weak passwords, pasting on monitors, hiding under keyboards, etc. These practices increase exposure to password compromise, but a multi factor authentication is the remedy.

A multi factor authentication (MFA) introduces an additional verification component to improve the security of the authentication function. A variant of MFA, the basic two-factor authentication (2FA) adds a second factor to compliment the password, and each time a user logs in using a password, a one-time credential is sent to the user's phone for instant verification. This feature should be turned on and made a mandatory security procedure particularly for remote work implementations.

3.2.5 Automatic notifications

The security settings of most connectivity devices come with notification functionalities that should be turned on. Relevant network traffic [8] and notifications trigger alerts when certain activities are attempted e.g. unauthorised information access, unauthorised alteration of password, suspicious insertion of account, etc.

3.3 Administrative and reactive controls

Administrative controls are work practice changes, procedures, and policies that lessen the threat of cyberattack. Reactive controls provide a response in the event of real or perceived attacks. They also include other pre-emptive measures that can forestall the likelihood of attacks.

3.3.1 Incident response

A pre-existing incident response plan is a must-have for every organization, so that in case a cybersecurity breach occurs, a robust action plan can be deployed to efficiently deal with the breach and get the organization back on its feet with minimum damage. An incident response plan should include a communications strategy for both internal and external stakeholders. Early preparation builds confidence for dealing with any crisis arising from WFH and other remote work implementations. It also boosts an organization's digital forensic readiness [9] [10].

3.3.2 Regular security briefing

A security briefing, as a cybersecurity routine, is a recommended practice where an organization provides information quickly and effectively about a trending cybersecurity issue. When delivered effectively as short written documents or presented in person, it can

influence decisions on technology use or offer solutions to user ignorance in the safe application of remote work implementations.

3.3.3 Routine data backup

Data backup is required to minimize monumental data loss that could arise from cyber breaches. There are many different types of backup systems, but they all have one thing in common, a spare copy of data is kept in a different location and treated as a fallback in case of loss of primary data.

3.3.4 Cyberattack simulation model

The proposed Randomized Cyberattack Simulation Model (RCSM) [9] is a checklist to ascertain the cyber defence preparedness of the organization to ensure readiness and familiarization with different forms of digital threats that can compromise vulnerable systems including WFH terminals. The model covers proactive protection in the following areas: malware, social engineering, denial of service, access control, cyber ethics, and cyber admin.

3.3.5 Cyber security policies

cyber security policies serve an essential purpose of specifying rules and guidelines for safe computing including guidelines for maintaining a secure experience in a telecommuting session. Adherence to such policies ensures that employees and users adapt with data loss prevention, strong passwords, software as a service (SaaS), managed services, etc. A policy statement for e.g. could indicate how multiple links can be set up to forestall insider collusion.

Policies relating to remote work systems should provide for strong identity authentication systems to forestall impersonation and to enforce multi-layered verification of legitimate personnel who are authorized to access classified data.

Furthermore, security policies must recognize and provide for defence in-depth as an approach whereby multiple levels of protection are deployed to guarantee greater levels of security.

3.3.6 Awareness

Employees need to be properly educated using appropriate information about the threats that are possible on telecommuting, video conferencing and other remote work channels including email phishing threats, social engineering scams and zoom bombing exploits. Proper awareness protects both the system and the users from the exploitative gimmicks of fraudsters.

4.0 CONCLUSION

The COVID-19 pandemic has reached a stage where working from home has become a norm. Globally, every organization has adjusted its work pattern, every economy is affected, and the

cybersecurity effects of WFH are huge. The biggest operational costs for organizations in the long run after staff wages and research will perhaps be cybersecurity.

Having previously identified insecure networks, capacity gap and social engineering as some of the significant risk factors for cyberattacks against telecommuting and video conferencing applications, this paper has proposed various solutions to mitigate the challenges. While maintaining vigilance, organizations should ensure that their remote work communications channels and terminals are protected with strong encryption technologies and intrusion detection and prevention systems, and that these systems are not outdated - including cloud services, Wi-Fi, web portals, devices, etc. Having a pre-existing good policy that specifies ethical standards and cybersecurity guidelines for employees is a sure way to enshrining quality preventive and detective controls. Above all, using a good antivirus software and endpoint solution that is fully up-to-date and functional is a plus.

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 Cybersecurity 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 Cybersecurity & 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] 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 29 May 2020].

[2] Ergic Cole, How to protect yourself against zoom bombing, Ashburn Virginia: Secure Anchor Consulting, 2020.

[3] Eric Cole, Work From Home Cybersecurity Guide: Preventing Cyber Theft for Remote Employees, Ashburn, Virginia: Secure Anchor, 2020.

[4] 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].

[5] P. A. Grassi, J. L. Fenton, E. M. Newton, N. B. Lefkovitz and Y.-Y. Choong, "Digital Identity Guidelines: Authentication and Lifecycle Management," National Institute of Standards and Technology (NIST) Special Publication 800-63B, Maryland, USA, 2017.

[6] SANS Institute, "Password Protection Policy," SANS Institute, Maryland, USA, 2017.

[7] SANS Institute, "Password Construction Guidelines," SANS Institute, Maryland, USA ,

2017.

[8] Sally Adam, "Five steps to avoid a cloud data breach," Sophos, 21 February 2020. [Online]. Available: https://news.sophos.com/en-us/2020/02/21/five-steps-to-avoid-a-cloud-data-breach/. [Accessed 31 May 2020].

[9] K. Okereafor and R. Djehaiche, "New Approaches to the Application of Digital Forensics in Cybersecurity: A Proposal," *International Journal of Simulation: Systems, Scienece and Technology (IJSSST)*, vol. 21, no. 2, pp. 36.1-36.6, 2020.

[10] 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.