International Journal of Advanced Trends in Computer Applications
www.ijatca.com

INFORMATION SECURITY IN A PANDEMIC

[1]Alebiosu Omobolade B.
[1]Computer Professionals (Registration Council) of Nigeria
[1]boladealeb@gmail.com

Abstract: *Organisations and individuals have embraced new practices such as social distancing and remote working as a result of the COVID-19 virus which was declared a pandemic by the World Health Organisation. Cyber criminals around the world capitalised on the crisis while the entire world focused on the pandemic, in particular the health and economic threats posed by COVID-19.Humans have always been the weakest link in cybersecurity, they are either carrying out the attack or the target of the attack. Individuals are increasingly the targets of two types of attacks: social engineering which seeks to circumvent an existing process and exposes an individual's lack of security awareness, while exposing obsolete/vulnerable software in a system or technology are the targets of logical engineering. Recent trends, according to cybersecurity statistics and which are also side effects of the global pandemic, reveal a huge increase in hacked and breached data from sources that are increasingly common in the workplace, like mobile and smart devices. Additionally, remote workforce greatly increased, giving room for cyber-attacks. This paper concludes that the pandemic introduced a new variation in cyber-attacks which majorly focused on; security risk from remote working/learning, malicious websites, mobile threats, malicious social media messaging and business email compromise, which might lead to the chances of downloading adware, spyware, ransomware and other malicious software. This paper also recommends that proper awareness on the new gimmicks of cybercriminals is essential inextinguishing the chances of a cyber-attack and possible information breach.*

Keywords: *Information security, cybersecurity, pandemic, cyber threats, covid-19.*

I. INTRODUCTION

The unprecedented circumstances surrounding the spread of COVID-19 virus has resulted in a shift towards adopting infrastructure to enable different services to be provided virtually. This shift technology adoption was necessary to minimize insufficiencies and maximize time and the quality of services rendered in different fields during the pandemic lockdown. The adoption of technology in several fields dramatically accelerated as result of restrictions imposed by several countries which altered the way work, continuous work and research was needed to ensure that the technological infrastructures adopted provides a safe and effective environment for everyone[1].

II. LITERATURE REVIEW

The origin and the evolution of the meaning of the term computer security did not just start recently years. Physical security of a computer was majorly all that was considered in the beginning when computer security was mentioned, but its meaning changed due to how widely publicized issues with data and information security became over time. Additionally, there are three reasons why computer facilities have been physically protected which are: to prevent theft of or damage to the hardware, to prevent theft of or damage to the information, to prevent disruption of service.

Computer security are the measures applied to computing devices such, as well as computer networkssuch as private and public networks, and the internet, computer security ensures that digital equipment, information and services are protected from unintended or unauthorized access, change or destruction by using approved processes and mechanisms. The possible security breach in line with the increasing reliance on computer systems explains the growing importance of computer security worldwide[2].

2.1 Information Security

Generally, security is defined as "the quality or state of being secure or to be free from danger." This means that

the purpose of security is protection against adversaries; which are those who pose a threat and would possibly do harm, intentionally or otherwise. For example, national security, uses a multi-layered system approach that protects the sovereignty of a state, its assets, its resources, and its people. Achieving the appropriate level of security for an organization also recommended to adopt a multifaceted system approach [3].

The evolution of information security began with computer security with the first mainframes. This arose from the need to secure physical locations, hardware, and software during the World War II, hence the need to implement multiple levels of security to protect these mainframes and maintain the integrity of their data. Access to sensitive military locations had a security measure emplaced, for example, they were controlled by means of badges, keys, and the facial recognition of authorized personnel by security guards. More complex and sophisticated computer security tools and mechanisms were developed to meet the growing need to maintain national security [4].

Information security is defined as the means of to protecting information, information systems and information assets as well as protecting its confidentiality, integrity and availability from unauthorized access, use, disclosure, disruption, modification, or destruction, whether in storage, processing. It is achieved via the application of policy, education, training and awareness, and technology [5].

Albert Caballero described information security as involving the protection of organizational data, information, operations, and assets from the disruption of business operations, modification of sensitive data, or disclosure of proprietary information. The protection of this data is usually described as maintaining the confidentiality, integrity, and availability of the organization's data, assets, operations, and information [6].

2.2 Pandemic

The Coronavirus Disease 2019 (COVID-19) was first spread and identified amid an outbreak of respiratory illness cases in Wuhan City, Hubei Province, China and was initially reported to the WHO on 31 December 2019. Subsequently, the virus spread to other parts of world and therefore, received worldwide attention. COVID-19is an illness caused by the novel coronavirus now called severe acute respiratory syndrome coronavirus 2 (SARS-CoV-2; formerly called 2019-nCoV). On 30 January 2020, the WHO declared the COVID-19 epidemic as a public health emergency of international concern and emergency. On March 11, 2020, the WHO declared COVID-19 a global pandemic [7].

COVID-19 is a global health crisis and also an international economic threat stifling and grounding all activities as a result of the worldwide lockdown of countries, businesses and several industries that were implemented in order to curb the spread of the virus. This resulted in a major shift from the traditional way work was carried out, and generated a wide array of unique and fundamental challenges for both employees and employers. Additionally, these restrictions did not just affect the industries but also the employees as they were turned overnight into work from home employees, essential or life-sustaining workers (this includes emergency room medical personnel, security and agro-produce sellers), or while some were laid off as their organizations were not working in the lockdown and could not meet up with the financial obligations. The lockdown equally affected organizations and related government activities as it changed some industries fundamentally, accelerated trends that were already underway in others, and it equally opened opportunities for novel ideas and industries to emerge[8].

2.3 How the Pandemic Has Affected How We Work

Organisations and individuals were forced to embrace the new practices as a result of the COVID-19 pandemic, these practices included social distancing and remote working. Governments reconsidered and implemented ways to ensure that their countries are stable by developing and enforcing new economic plans. Nevertheless, cyber criminals around the world capitalised on the crisis while the entire world focused on the pandemic, in particular the health and economic threats posed by COVID-19 [9].

Remote work also known as work from home or telecommuting is claimed not be a new term to use in nowadays, it is said to have been around for longer than 10 years, but was made popular as a result of the pandemic. The COVID-19 pandemic bound most employees globally to work from home no matter the preparedness level of the organisation,the pandemic made this an impulse decision instead of a choice. Firms that deal with a lot of confidential client information will have to ensure that employees are working from a secure environment when they work remotely by providing secure connections to their platforms. The first step here is to install the right security software and enable automatic updates, not just on laptops, but also on smart phones or any other personal devices that employees might use to access client data [10].

Delloite Nigeria's Cyber Intelligence Centre's report, stated that was a spike in phishing attacks, mailspams and ransomware attacks as attackers are using COVID-19 as

bait to impersonate brands thereby misleading employees and customers, who might unknowingly visit the malicious website or download such contents. This will likely result in more infected personal computers and phones. The report stated that not only businesses targeted, end users who download COVID-19 related applications or contents were also tricked into downloading ransomware disguised as legitimate applications [9].

III. METHODOLOGY AND ANALYSIS

This research paper aims to present a deeper insight to analyze the impact of COVID -19 on the information technology field particularly information security.This research paper is basically descriptive and analytical in nature. Data collection is based on secondary data. Secondary data is collected from survey reports conducted by information security consultants and a number of industry top level companies in information technology, this data is also based on the current data and scenario. The secondary data is collected from various survey reports, research papers, articles and publishing of 2020-2021 year according to the need of the study.

IV. DISCUSSION

4.1 Cybersecurity Threats in A Pandemic

Increased security risk fromremote working/learning

In a survey by IBM and morning consult conducted on professionals new to working remotely, thereport s stated that survey of finds those employees pose serious security risks—and it may not be their fault. With many employees working from home and students learning virtually, enterprise virtual private network (VPN) servers have now become a lifeline to companies/ schools, and their security and availability will be a major focus going forward [11]. In a bid to achieve this, there is a possibility that an organisation's unpreparedness will lead to security misconfiguration in VPNs thereby exposing sensitive information on the internet and also exposing the devices to Denial of Service (DoS) attacks.In addition to this, the use of personal computers to perform official duties by some users posed a great amount of risk to organisations. Organisations were advised to ensure VPN services are safe and reliable, and to equally advise employees against the use of personal computers for official purposes [12].

The report surveyed more than 2,000 people new to working at home due to the COVID-19 pandemic, and found that while 80% are confident in their organization's ability to handle cyberthreats that arise due to remote work, 45% also said that they haven't received any additional security training since going remote. IBM's study mirrors other findings about the state of cybersecurity during the pandemic, specifically that it's not keeping up by largely failing to provide security tools necessary to keep remote workers safe [11].

KPMG in her report stated that not all organisations were technically prepared to offer remote working options. As time pressure did not allow some IT staff acquire and offer most secure solutions. The report encouraged the use of multi-factor authentication for access to company data, along with secure and solid cloud solutions for collaboration where possible. While some companies temporarily offered their collaboration solutions for free, companies such as Microsoft Teams, Google Hangouts Meet, LogMein Emergency Remote Work Kit, Cisco Webex etc [13].

Malicious Websites

There has been an increase in websites that claim to be applications that are supposed to protect users from COVID-19, such as www.antivirus-covid19.site and www.coronaantivirus.com. According to Malwarebytes' blog, the website www.antivirus-covid19.site is now inaccessible. The website www.corona-antivirus.com mentions that their application, called "Corona antivirus," has been developed by scientists at Harvard University. But in reality, installing this application infect the system with a malware called BlackNET RAT. This malware makes the infected devices work as a botnet. This can help to launch a DDoS attack, upload some remote files, execute malicious scripts, collect browser cookies and passwords and harvest keystrokes, etc. [14].

Mobile Threats

In this modern era of ubiquitous computing, smartphone users are at their peak. Life without smartphones and gadgets has become impossible, and the use is increasing on a daily basis. At the same time, it's a great opportunity for bad actors to take advantage of it. An application named CovidLock (Ransomware) comes from a malicious Android app that is supposedly helping to track COVID-19 cases. The ransomware locks victims' phones, who are given 48 hours to pay USD100in bitcoin for recovery. Threats include the deletion of the phonedata and the leakage of the account information in social media [14].

Skybox Security published the mid-year update to its 2020 Vulnerability and Threat Trends Report. The report revealed that the volume of mobile vulnerabilities has increased by 50 percent. This increase is wholly driven by new Android deficiencies (which increased by 110 percent from 230 last year to 484 this year), after the number of new iOS vulnerabilities dropped by 23 percent from 152 to 117. In previous years such an increase may not have concerned security leaders, but after COVID-19 pandemic blurred the line between corporate and domestic spaces it underlines the importance of securing all possible access points, says the report [15].

Users still aren't securing their accounts properly. When they're carrying phones that contain both company accounts and personal sign-ins, that can be particularly problematic. A survey by Google and Harris Poll found just over half of Americans reuse passwords across multiple accounts. Equally concerning, nearly a third aren't using 2FA (or don't know if they're using it — which might be a little worse). Only a quarter of people are actively using a password manager, which suggests the vast majority of folks probably don't have strong passwords in most places, since they're presumably generating and remembering them on their own [16].

Malicious Social Media Messaging

Nowadays, social media is very common and is almost in the reach of every individual. Hackers find it a great opportunity and tend towards the various social media platforms such as Facebook and WhatsApp. There have been numerous cases in which scams and phishing tactics are circulating on Facebook Messenger and many other such applications. The scams typically lure victims into free subscriptions such as Netflix premium free account. When the victim clicks on the link, it redirects them to their social media phishing website. In some cases, it may ask to enter the credentials of their accounts. This way, they either capture their credentials or install malware into their systems, mobile devices, and web browsers to steal information and cookies, and thus, the user becomes a victim [17].

Business Email Compromise

Agari Cyber Intelligence Division reported a Business Email Compromise attack as the intruders took advantage of COVID-19. The attack was carried on by the Ancient Tortoise, a cybercrime organization behind several BEC cases in the past. This attack is believed to be a series of the previous attacks the group launched earlier. The attackers first target the bank accounts [18]. Then they use the information of the customers and send them emails to change their bank information and payment methods due to the novel coronavirus. The attackers pretend to be from legit organizations or businesses. In the current situation, the business email compromise scams are using coronavirus disease as a tool. The scam works by convincing or tricking the targets into making transactions to an intruder who shows him/herself as a legit employee working in the same company [16].

Phishing is the scam by which an e-mail user is duped into revealing personal or confidential information which the scammer can use illicitly [19]. This type of attack has gone beyond the use of email and has increased gradually during this period of Covid-19. Attackers are now using SMS and phone calls to retrievevictim's confidential information such as login details (usernames, passwords, pins among others). Moreover, confidential or sensitive information of users can easily be obtained when they visit fake websites or download documents from insecure sites.

4.2 Importance of Information Security

As part of the measures to fight against cybercrimes in Nigeria, the National Information Technology Development Agency (NITDA) advised Nigerians on the importance of data backup as mitigation strategy during this era of COVID-19. The recommended guidelines are highlighted: Ensure you backup your data frequently and at relevant intervals;Consider using remote storage for your backups;Ensure that the files containing your data backups are encrypted and protected; andUse multiple methods and multiple media for your data backups [20].

The modern cybersecurity environment has become incredibly diverse. To reduce risk and improve security posture across all network elements, organizations need to operate with a single view of compliance and operational security processes that can be aligned across the entire estate — including on-premises, OT, third-party and cloud networks. Through automating data collection, correlation and analysis, security and IT teams can together leverage a visual, interactive network model to understand risk levels, simulate attacks and remediate where it's needed most [15].

Organizations need insight that allows them to stop breaches before they happen. This can only be achieved when they understand how exposed their vulnerabilities are to attack. By modeling the environment in which a vulnerability occurrence exists, teams can understand the exposure of vulnerabilities to threat origins — a critical

component of risk-based vulnerability prioritization [21].In light of these increasing risks, organisations should take greater care when it comes to cybersecurity. The first step is reminding yourself and your co-workers of company cybersecurity protocols. The chaos of the outbreak can be distracting, so ensure everyone at your firm maintains safe internet behaviour. You should always pay attention to suspicious emails, but it's even more crucial now. Double-check anything you receive that mentions coronavirus, as these links are far more likely to be fake. Even mail from a seemingly credible source could be a trap, so inspect everything. It's also essential to ensure all personnel have access to the right security tools. When you're working with sensitive legal documents, you can't risk a data breach. Make sure everyone at the firm or office can access company cybersecurity software, even from home [22].

Working from home can feel more casual than an ordinary day of work, but you shouldn't let this relaxed atmosphere lull you into poor security habits. Only use your company email to discuss sensitive information like client data or financial records. Additionally, your firm should embrace a data breach response plan if you don't already have one. If you are the victim of a cyberattack, you should have a protocol in place to handle the situation.

For many years, the concept of fear, uncertainty, and doubt (FUD) has been discussed in the cybersecurity arena, which has helped to implement information security technologies. The detail that must be grasped in relation to the success of this concept is that, in a world where information technology created isolated systems or systems connected with other systems via specific points, defence systems such as antivirus software, firewalls, etc. were the solution to the main problems of electronic security and theft of confidential information [23]. In recent years, with the advent of technologies that form the work environment known as Industry 4.0, in a hyperconnected world where systems have come to form ecosystems, to continue using the FUD principle would be a mistake that could deepen the crisis. This is because such an approach could increase the technological inequality between those who implement these changes and those who do not, leaving out of the fourth industrial revolution those institutions that out of fear do not implement technological solutions as a driver of operational efficiency. The biggest risk in a hyper-digitized and hyperconnected world is failure to take technological risks.

V. CONCLUSION

In the post-COVID-19 world, cyber attackers are increasingly seeking to exploit vulnerabilities in an organisation's security infrastructure that the shift to remote working has exposed. It is time for cybersecurity leaders to re-visit their security measures and focus on deploying new processes and technologies to fortify their digital architecture going forward. Recent trends, side effects of a global pandemic and cybersecurity statistics reveal a huge increase in hacked and breached data from sources that are increasingly common in the workplace, like mobile and IoT devices. On top of this, COVID-19 has ramped up remote workforces, making inroads for cyber-attacks [24].

In an increasingly digital and connected world, with disruptive technologies and demanding implementation times, exposure to a cyberattack is only a matter of time. The effort must then be made to lower the chances of occurrence by means of a cybersecurity management plan that includes effective measures in relation to processes, technology and people, regardless of the size of the organization, while at the same time preparing as well as possible to deal with an incident.

This paper concludes that the pandemic introduced a new variation in cyber-attacks which majorly focused on; security risk from remote working/learning, malicious websites, mobile threats, malicious social media messaging and business email compromise, which might lead to the chances of downloading adware, spyware, ransomware and other malicious software. The panic and anxiety associated with the coronavirus have increased online vulnerabilities and ignited a wave of cyberattacks using social engineering as a tool, whereby cybercriminals are taking advantage of human fear and apprehension to distribute destructive codes in the guise of authentic coronavirus information and stealing confidential information in the process [25]. This paper also recommends that proper awareness on the new gimmicks of cybercriminals is essential in extinguishing the chances of a cyber-attack and possible information breach.

REFERENCES

[1] Mohammad S. Jalali, Adam Landman, William Gordon. (2020) Telemedicine, Privacy, and Information Security in the Age of COVID-19 SSRN-id 3646320.

[2] Sumitra Kisan, Chandrasekhar Rao. Veer Surendra Sai University of Technology, Information Security Lecture Notes.

[3] CourseHero. Computer System Security - Foundations of Computer Security, accessed https://www.coursehero.com/file/49810076/Computer-System-Security-1docx/ on 4 March 2021.

[4] Michael E. Whitman, Herbert J. Mattord. (2018) Principles of Information Security, 6th Edition.

[5] Wikipedia. Definition of information security, accessed http://en.wikipedia.org/wiki/Information_securityon 4 March 2021.

[6] Albert Caballero. (2013) Information Security Essentials for IT Managers: Protecting Mission-Critical Systems, Terremark Worldwide, Inc.

[7] David J Cennimo. What is COVID-19? Mar 03, 2021, Medscape Publication Thursday, accessedhttps://www.medscape.com/answers/2500114-197401/what-is-covid-19 on 5 March 2021.

[8] Kniffin, Kevin & Narayanan, Jayanth &Anseel, Frederik &Antonakis, John & Ashford, Susan & Bakker, Arnold & Bamberger, Peter &Bapuji, Hari &Bhave, Devasheesh& Choi, Virginia &Creary, Stephanie & Demerouti, Evangelia & Flynn, Francis & Gelfand, Michele & Greer, Lindred& Johns, Gary &Kesebir, Selin & Klein, Peter & Lee, Sunyoung&Vugt, Mark. (2020). COVID-19 and the Workplace: Implications, Issues, and Insights for Future Research and Action. 10.31234/osf.io/gkwme.

[9] Deloitte Nigeria. (2020) Covid-19 Impact on Cybersecurity

[10] Meenakshi Kaushik Neha Guleria. (2020) The Impact of Pandemic COVID -19 in Workplace, European Journal of Business and Management, ISSN 2222-1905 (Paper) ISSN 2222-2839 (Online) Vol.12, No.15.

[11] IBM Security, Morning Consult. (2020) IBM Security Work from Home Study accessed http://filecache.mediaroom.com/mr5mr_ibmnews/186506/IBM_Security_Work_From_Home_Study.pdf on 4 March 2021.

[12] Brandon Vigliarolo. Employees new to working remotely are a security risk June 22, 2020, accessed https://www.techrepublic.com/article/employees-new-to-working-remotely-are-a-security-risk/ on 4 March 2021.

[13] KPMG. (2020) Coronavirus and Cyber Security Report.

[14] Navid Ali Khan, Sarfraz N. Brohi, Noor Zaman. (2020) Ten Deadly Cyber Security Threats Amid COVID-19 Pandemic.

[15] Skybox Security, Vulnerability and threat trends report, 2021. [Online]. https://lp.skyboxsecurity.com/WICD-2021-02-Vulnerability-Threat-Trends-Reg.html Accessed on 5 March 2021.

[16] Raphael JR. 8 mobile security threats you should take seriously, MAR 1, 2021 [Online].https://www.csoonline.com/article/3241727/8-mobile-security-threats-you-should-take-seriously.html [Accessed: 4 March 2021].

[17] David Marques, Data Security and Privacy in Times of Pandemic, proceedings of the Digital Privacy and Security Conference, 2020.

[18] Peterson P, "Business Email Compromise (BEC): Coronavirus a Costly New Strain of Email Attack," 2020. [Online]. Available: https://www.agari.com/email-security-blog/business-emailcompromise-bec-coronavirus-covid-19/. Accessed on 6 March 2021.

[19] Mariam-Webster, Definition of phishing,2021. [Online].https://www.merriam-webster.com/dictionary/phishing. Accessed on 6 March 2021.

[20] Onwuaso Ugo, COVID-19: NITDA advises Nigeria on data backup as impact mitigation strategy' 2020. [Online]. Nigeria Communications Week https://nigeriacommunicationsweek.com.ng/covid-19-nitda-advises-nigerians-on-data-backup-as-impact-mitigation-strategy/ Accessed on 7 March 2021.

[21] Skybox Security, 2020 Vulnerability and threat trends mid-year update, 2020. [Online]. https://www.skyboxsecurity.com/wp-content/uploads/2020/07/2020-VT_Trends_Executive_Summary.pdfAccessed on 6 March 2021.

[22] American Bar Association, The Importance of Cybersecurity Amid COVID-19, 2021. [Online]. https://www.americanbar.org/groups/law_practice/resources/cybersecurity_covid19/accessed on 7 March 2021.

[23] Sony Anthony KPMG-The importance of cybersecurity in the post-COVID-19 world, 2020.

[24] MICROPAC, 5 Trends Expected to Dominate the Cybersecurity Scene In 2021, 2021 https://micropactech.com/main/5-trends-expected-dominate-cybersecurity-scene-2021/ accessed on 7 March 2021.

[25] Kenneth Okereafor, Olajide Adebola, Tackling the Cybersecurity Impacts of The Coronavirus Outbreak As A Challenge To Internet Safety, International Journal in IT &Engineering, Volume 8, Issue 2, February 2020.