THE INTERNATIONAL JOURNAL OF SCIENCE & TECHNOLEDGE

COVID-19 Pandemic and Cyber-threat: A Major Concern in Q1 of 2020

Anene Nduka
Consular Assistant, Department of Consular,
Nigeria High Commission, Malaysia
Abubakar Umar
Consular Secretary, Department of Consular,
Nigeria High Commission, Malaysia
Ogbechie Okwudili Patience
Ph.D. Candidate, Department of Public Administration,
Nasarawa State University, Nigeria
Abba Mustapha Mohammad
Ph.D. Candidate, Department of Business Management,
Limkokwing University of Creative Technology, Malaysia
Umar Umar
Masters Candidate, Department of Computer Science,
Nigeria Defence Academy, Kaduna, Nigeria
Maikarfi Ramlat Ibrahim
HR Secretary, Department of Human Resource, Bionas Nigeria LTD, Nigeria

Abstract:
The emergence of COVID-19 pandemic has threatened the existence of our humanity, civilization, as well as had a great impact on our cyber security. As tech giants and government are taking an opportunity to advance their digital surveillance while criminals are taking advantage of the situation to perpetuate their nefarious acts. The lockdown of global economy due to the emergence of coronavirus necessitated the migration to digital infrastructure, as individuals and cooperate bodies depend on it for their daily business, research, and entertainment. The cyberspace has witnessed a deluge of information overload, as well as fake news, which is creating panic and misinformation among human population and allowing cybercriminals take advantage of the situation. It is imperative to join hands in sanitizing our cyberspace, take appropriate cyber security measures, respect privacy and ethical boundaries and be vigilant while surfing the internet. We are currently not fighting to combat only coronavirus pandemic but also cybercrime, economic meltdown, fake news which has led to outright disregard of precautionary measures, leading to fatalities, panic, and vulnerabilities on a global scale.

Keywords: *Infodemics, Cloud, Internet, Cybersecurity, Coronavirus, Phishing, Malware, Zoombombing*

1. Introduction

Human beings as social entities, thathave always devised various means of communicating with each other, which ranges from simple pictures (petroglyphs), symbols, alphabets, electromechanical and the internet. Evolution of our information technology has sharpened the way we communicate with each other, how data can be generated, stored, and transmitted in real time, irrespective of the distance. The digitalization of information triggered the rise of digital platforms and applications that are used in diverse spheres of life. As the world today is experiencing a cataclysmic impact of coronavirus pandemic which has triggered a surge in the use of internet for various reasons during this lockdown and as such attracted the attention of different quarters to unleash mayhem to unsuspecting users.

As Social distancing continue to caused economies to bleed worldwide (Abubakar et.al, 2020),organizations, businesses, agencies and governments have migrated their operations/services to the cloud while their staff are granted access to their domain, which enable them to work from home with the help of various tools, platforms and applications. The cascading pandemonium caused by COVID-19 pandemic and its global impact is making cybersecurity critical as people become more dependent on digital infrastructure for various reasons. The current pandemic is accelerating the trend of global economic and social dependence on the internet (Weforum[1], 2020).

In this research, we explore the impact of cyber security, digital surveillance, and deluge of information during the outbreak of coronavirus. We will examine different tools, platforms, applications that are used by cyber criminals to perpetuate their nefarious acts. The impact of cybersecurity breaches on individuals, organizations, and global economy,

as well as efforts to combat this insurgence. We shall be focusing on different types of cyber attacks being perpetuated by cyber criminals regarding COVID-19 pandemic.

Cyber criminals have employed different tools and approaches to defraud their victims and Phishing is the most used tool. They are taking advantage of panic created by this COVID-19 pandemic to prey on people's emotion and concerns for urgent information and necessary supplies. They send unsolicited malware-laden-emails about the virus, its prevention, fake cure, and statistics, as well as advertise for face mask and personal protective gears on fake domains (Ahmad, 2020).

We have learned that certain measures, such as social distancing, isolation, personal hygiene, use of face mask in the public, should be taken to reduce the risk of coronavirus. We equally need to upgrade our cyber security hygiene by adopting measures such as the use of antivirus, strong passwords, and avoid clicking links, infodemics as well as visiting only trusted sites, and adverts that are too good to be true.In this time of digital dependency, cyber criminals are taking advantage of this pandemic to bait unsuspecting individuals by sending them unsolicited messages with malicious attachments or links that can compromise their cyber security, this approach is known as phishing (WHO, 2020). Being acquainted with cybercriminals modus operandi will help to reduce the risks of being a victim and try not to download files or follow links from unfamiliar people, (Mauro, 2020).

Internet users should always be on the lookout for the following tips to identify phishing scams, and they are viz: email asking for clicks, fake domain or websites, messages claiming to be from official source or the CEO, unrealistic advertisements and rates, bogus email address and sites, no security certificate for domains and websites, grammar and spelling error, malicious links or harmful attachments, messages requiring urgent action (Ahmad, 2020).

According to the United Nations, cyber security is critically important in times of these crises of infodemics and coronavirus, stressing that vast majority of the world population have migrated their studies, businesses and jobs to the cloud due to the lockdown, thereby making them susceptible to cybercrime (UN, 2020). Organizations are racing to educate their staff about cyber security to avoid being victims of this onslaught of cybercrime. (Ahmad, 2020).

1.1. Hypothesis

- H1. People are not fully aware of the impact of coronavirus on cybersecurity.
- H2. The lockdown necessitated virtual collaboration/video conferencing thereby forcing organizations to adopt low-grade or consumer-grade video conferencing platform used from home.
- H3. Not all online users are aware of cybersecurity threats and the modus operandi of cybercriminals, hence the need for public awareness campaign to safeguard digital infrastructure of individuals, organizations, and businesses.
- H4. Digital surveillance by tech giants and governments will continue to rise despite privacy and ethical concerns.
- H5. Adoption of technology will continue to increase despite threats of cybersecurity.

1.2. Research Methodology

In this research, we adopted quantitative research method due to domestic movement control order/lockdown imposed by the governments and the closure of international borders in most countries, which makes it impossible to generate primary data from direct respondents. Alternatively, we will be focusing on cooperate reports, contemporary literature, online publications, professional empirical documented works, and opinions related to coronavirus pandemic and antecedent cyber security challenges, which will be reviewed to generate our data. This research studies deeply the experience, preparedness, impact and intentions of governments, health agencies, big tech organizations and experts in the face of this coronavirus pandemic and cyber security challenges associated with the mandatory stay at home imposed by various governments across the globe. Finally, the chosen methodology entails comprehensive and analytic inference that is robust in addressing trends, data collection, phenomenon, and characteristics, which makes it more suitable for this research.

2. Literature Review

As coronavirus pandemic continues to ravage our global health, social, economic, and political systems, another unseen monster now threatens our cyberspace, which prey on our increased reliance on digital infrastructure (Weforum[2], 2020). The World Economic Forum's 2020 Global Risk Report in January 2020 before COVID-19 pandemic was known to the world, predicts that cybercrime damages in the U.S alone, might reach $6 trillion by 2021. It was also reported that in the month of April 2020, 89 U.S. based organizations were confirmed to have been attacked by cybercriminals but recorded a low success rate (Barth, 2020).

The new trend of working from home due to the lockdown was triggered by emergence of coronavirus pandemic, which has stretched the cyber security of organizations, governments and individuals to its limits, as most of these devices used at home are not fully protected. It is reported by Absolute 2019 Global Endpoint Point Security Trend that, 42% of devices connected to the internet are unprotected at any given time (Ahmad, 2020).

According to Ahmad (2020), there has been a spectacularly spike in cyber-attacks by criminals, suggesting that cyberattack attempts reached 145 cases per 1,000 endpoint devices, between February 23, 2020 to April 4, 2020 as compared to 37 attempts before February 22, 2020. He further stated that cybercrime will cost the world about $6 trillion annually by the end of 2021. About 4,000 COVID-19 domains have been registered this year and of whom majority of them are from cybercriminals, as they continue to capitalize on our fear and ignorance to unleash mayhem. They clone or infect e-commerce platforms to target victims trying to buy medical or essential supplies (Ahmad, 2020).

While all these are going on, several cybercrime gangs have promised to halt their attacks on healthcare organizations, nursing homes and 911/emergency services during this pandemic. One gang promised to continue their nefarious activity against big pharmaceutical companies who are taking advantage of this pandemic to make money, while other ransomware operators promised to offer free decryption services for hospitals, they mistakenly encrypted (Hope, 2020).The World Health Organization (WHO), Center for Disease Control and Prevention (CDC), the United Nation (UN) and other local and international health organizations are facing increasing attacks and impersonation by cybercriminals to perpetuate their nefarious acts, such as phishing attacks and inserting malware into online resources for tracking the pandemic (Umeh, 2020).

It is reported that a total of 556 cases of face mask scams were recorded in Malaysia alone, out of which 501 cases occurred between March 18, 2020 and April 3, 2020, resulting in RM3.5 million loses in Malaysian currency. Their modus operandi is to lift face mask adverts from genuine company and e-commerce domains then use it to advertise on other social media and other e-commerce platforms, such as Facebook, WhatsApp, WeChat, Mudah.com, Shopee andInstagram (Zolkeple, 2020).

Another report by The Star Malaysian newspaper publication, suggests that cybersecurity related cases rose by 82.5%, which amounted to a total of 838 reported incidence from March 18 to April 7, 2020. This increase was due to the lockdown imposed by the government. Which invariably increased dependence on the internet for business activities, online banking other related transactions and social media platforms for virtual conferencing, education, and leisure (Meikeng, 2020).

Report from Action Fraud, (UK's reporting Centre for fraud and cybercrime), shows that the United Kingdom alone has lost over £2 million to coronavirus online phishing scam while their United States counterpart, Federal Trade Commission said, 'Americans have lost over $12 million to coronavirus scams since January 2020, with over 16,800 reported cases' (Palmer[2], 2020).

While cyber criminals are having their filled day, governments across the world, agencies, organizations, internet service providers and technology firms, are intensifying efforts to curb the activities of these criminals. Thousands of fake domains have been dropped, as well as fake news circulating on Facebook and Instagram has been debunked and brought down, while over two billion guests have been rerouted to accredited agencies domain (Tidy, 2020). Fortunately, payments to cybercriminals are incredibly low, since we all live in the same reality of global lockdown caused by COVID-19 pandemic.

2.1. Types of Cyber-attacks

In this research, we will be focusing on different types of cyber attacks that are being perpetuated by cyber criminals with regards to COVID-19 pandemic.

- Malware: Also known as malicious software or program, designed to steal personal data, damage computer device, server, client, computer network and alter the functionality of a computer system.
- Phishing: Impersonating individuals, organizations, or government agencies with the intention to defraud people or steal their personal data
- Spamming: Sending unsolicited mails, advice, adverts, and promotions with malicious attachments to people with the intention of defrauding them or stealing their personal data by installing key loggers.
- Ransomware: Described by the US Department of Justice (DOJ), as 'a new business model for cybercrime' and a global phenomenon. Infects computers, restrict access to files, hijacking of database, server, services, or digital resources and demanding a ransom before restoring it back.
- Social engineering: Impersonation with fake credentials to gain access to individual/organizational database or requesting victims to call, message or visit certain websites that requires them to divulge sensitive information or support nonexistent charities.

2.2. Virtual Conferencing

As the name implies, it is an online meeting platform/app which enables individuals to communicate and share digital contents over the internet in real time. Certain virtual conferencing apps can accommodate between few to hundreds of users at once, while instant chats, video/audio, digital file sharing and webinars across multiple platforms are permissible. Working from home due to this lockdown has warranted an unprecedented demand for virtual collaboration, hence forcing organizations to adopt low-grade or consumer-grade video conferencing platforms/packages, as well as the use of unprotected devices for official purposes which could cause potential security risks (Ahmad, 2020).

As virtual conferencing apps and platforms are witnessing a surge in downloads, sign-ups, and usage, it has become a hotbed for cyber criminals to perpetuate their nefarious acts. For the sake of this research, I will be focusing on the following virtual conferencing apps and they are: Zoom, Google Hangout and House party.

2.2.1. Zoom

Founded in 2011, is one of recent and leading social media enterprise that provides certain cloud platform services, such as video/audio conferencing, instant chats and webinars across multiple platforms and compatible with all devices, such as, laptops, desktops and mobile devices. It is credited with the capacity to accommodate up to a 100-users, with high quality, face to face video and instant messaging. The application has suddenly become more popular due to the emergence of coronavirus pandemic that forced everyone to stay at home thereby increasing the demand for virtual collaboration and conferencing.

According to The Star Malaysian publication, thousands of Zoom video call recordings have been exposed on the open web. Which can be accessed and downloaded through an open online search, because naming of Zoom recordings is identical, thereby making it too easy to guess. It was also reported that these videos can be found in unprotected section of Amazon storage space, known as 'buckets', which has been uploaded on sites like Vimeo, YouTube, and other free online search engines. Using Zoom default naming pattern yielded over 15,000 result at once and the video recordings were not protected (Yeoh, 2020).

An incident which occurred in Singapore, where an online class on zoom platform, was hijacked by hackers who displayed pornographic content, before requesting the girls to bare their chests, resulted in the suspension of Zoom in the country, pending the security loopholes being fixed (MalayMail, 2020). Individuals, academics, organizations and government meetings across the world have continued to endure abusive Zoom bombings in series of incidents which include, child abuse, pornography, racial slurs, as well as previously recorded videos lasting hours in the open cloud even after being deleted by users (Hodge, 2020). A CNN Business news suggests that zoom is sharing user's data such as language, time zone, IP address and device model number with Facebook, without users' consent. They only provide transport encryption which only secures the message during transmission, as against their promise of end-to-end encryption (Lyengar& Fung, 2020).

According to Bleeping Computer report, about 530,000 Zoom accounts which include email address, passwords, personal meeting URL and their HostKey, were purchased from the dark web and hacker forums for less than a penny, by Cyble. Amongst these recovered accounts belonging to individuals and well establishes cooperate organizations, such as Citibank, Chase, educational institution. In line with the forgoing, Zoom in a statement stated that'they have hired multiple intelligence firms to find these passwords dumps and the tools used to create them', and promised to continue their investigation on the subject matter, while asking users to change their password and promised to bolster their security apparatus (Abrams, 2020).

2.2.2. Google Hangout

As the name implies, it is a free communication software developed by Google in the year 2013, which enable users to make video, audio call, chat and send instant messages and files. The app is compatible with all platforms and devices and can accommodate up to 150 users at a time. Users are required to register a Gmail account which comes handy with the app and users are required to sign-in to their Gmail account before they can use the app.

It is reported that Google is blocking an average of 240 million COVID-19- related phishing messages daily. This proactive measure is to stop cyber criminals from stealing user's personal information, identity theft, and impersonation of health agencies such as WHO. Put a stop to duping users into donating to a fraudulent account or luring them with lucrative but fake business deals regarding the pandemic.

In the light of the forgoing, Google has optimized its G Suit's advanced phishing and malware controls, which are automatically turned on by default (Tung, 2020).Since Google hangout is linked with users Gmail account, conference convener or admin can easily add only invited guest to the chat room but does not provide advance settings. It is user friendly, and seamlessly synchronized with other Google products, as well as continuous improvement and updates. On the other hand, users can add a third-party to the chartroom by sending them the chat room link.

2.2.3. House Party

This is a free social networking app which is used across multiple platforms and compatible with mobile and desktop applications, that enable video chat amongst several individuals in real time. The emergence of COVID-19, has triggered unprecedented increase in download and use of the app. A BBC report suggests that the app recorded a rinse in downloads from 130,000 per week in mid-February, to2million downloads per week in mid-March 2020 (BBC, 2020).
There have been rumors circulating in the media and several posts on Twitter by users claiming the hijack of their accounts and being locked out of certain other applications, which include, Spotify, Netflix and even their bank account, after the download of the House party app. This led to House party owner offering a $1 million bounty to prove the credibility of such claim (BBC, 2020).

3. Global Impact of Cyber Security Breaches

The emergence of coronavirus pandemic has witnessed a dramatic rise in cyber attacks with more precision, sophistication, stealth, devastation, and tenacity of cyber criminals. Individuals, businesses, cooperation's, and governments across the globe have in this first quarter of 2020 been victims of one or several cyber attacks ranging from data breaches, loss of money, intellectual property, confidential records, business disruptions and reputation damages. It is estimated that ransom are attacks occur every 14 seconds and usually lunch through online phishing approach and could cost businesses an estimated $11.5 billion globally by the end of 2020 while the figures could rise to$20 billion by 2021 (KPMG, 2020).

According to IT governance publication, a total of 8.8 billion records were breached only in the month of May 2020 while about 216 million records were breached in the month of April 2020. It was reported that energy giant EDP (Energias de Portugal) became a victim of a ransomware attack that affected 10 terabytes of its data, as the criminals demanded about €10 million ransom to be paid through Bitcoin (Irwin, 2020). A group of hackers have published hundreds of thousands of potentially sensitive files belonging to over 200 police departments and FBI offices across the US which is searchable by officers' badge numbers. The leaked files reveal that the police, FBI and other law enforcement

agencies are using social media platforms to monitor and profile people in the wake of protests against George Floyd's death (Platt, 2020).

Cyber criminals are cashing in on the disruption caused by COVID-19 pandemic by preying on businesses and supply chain industry's vulnerabilities such as weakened approval process, reduced workforce working from home, shortages of goods and services, fear, uncertainties and poor oversight to unleash mayhem on both businesses and individuals. This is achieved by intercepting communication between buyers and sellers and rerouting payments to their bank accounts or the use of fake email accounts and social engineering approach to impersonate legitimate business and accepting payments from unsuspecting customers without delivering any goods or services. The First Quarter (Q1) of 2020 has witnessed a fivefold increase in cyberattacks, as criminals are taking the advantage of coronavirus pandemic and the loopholes that it presents.

3.1. Digital Surveillance

The emergence of COVID-19 pandemic which disrupted the activities of individuals, businesses, and governments, created an avenue for states to advance their digital surveillance despite efforts by human right organizations and allied organizations to expunge cyber espionage/surveillance. With the world racing to develop vaccine and treatment for coronavirus, pharmaceutical firms and research institutes involved in this research have increasingly become targets for cyber espionage by certain governments that want access to this cutting-edge intellectual property (Fidler, 2020).

Several governments and tech-giants across the globe are capitalizing on the COVID-19 pandemic to advance their digital surveillance on its citizens or users. According to a BBC News report, UK citizens will soon be asked to track their movements through their smartphones or Bluetooth-enabled wristband, to help curtail the spread of coronavirus. It reported that the UK government is deploying 18,000 workforces to track the contacts of those infected and the people they had contact with, will be asked to go for testing or self-quarantine (Lawrie, 2020). Across the globe and in countries like China, Israel, India, Singapore and the entire Europe, governments have embraced the emergency measure of data collection through CCTV cameras, credit card transactions and mobile phones to track infected patients and others they might have come in contact with (Ben-Hassine & Dawson, 2020).

South Korea is taking a step further by tracking their citizens via mobile phones, to tracking their credit card usage and CCTV footage, to ascertain their movement and people they probably had contact with. Advanced surveillance by various governments and tech-giants have triggered skepticism from individuals and various human right organizations about public security and online privacy. While the UK government agencies and tech-giants, have pushed back by assuring individuals about the safety of the app, and promised data gathered will only be used for health and research purposes, while the app can be deleted at any time (Lawrie, 2020).

Authorities and big-tech organizations across the globe are deploying various technologies, devices, and tools such as AI. Surveillance cameras, drones, IoT, Bluetooth, Radar technology, smart phones, the internet, and mobile network in disguise of Covid-19 surveillance to advance their surveillance on its subscribers/citizens which will outlast this pandemic (Anene et.al. 2020).

3.2. Rise in Online Scam, Bank Scam

There has been a rise in banking scams during this pandemic, where fraudulent individuals who claim to be employees of various banks in Nigeria, are making phone calls to people, requesting their bank details to facilitate the disbursement of federal government COVID-19 relief package. It is reported that these fraudsters will provide customers with their personal details such as their Bank Verification Number (BVN), name and date of birth, so as to gain the individuals confidence to release their ATM PIN number. On another note, criminals are impersonating banks by sending emails to unsuspecting customers informing them about the soon expiration of their bank token device and advising them to urgently click certain link to visit a webpage so as to reactivate of synchronize their accounts, to validate their transactions and avoid their accounts being frozen(Zenith Bank, 2020).

It has been reported according to ZDNet, that North Rhine-Westphalia province in Germany is believed to have lost millions of euros to cyber criminals after they cloned their website set up to distribute COVID-19 financial aid and lured citizens through email campaigns to provide their data. They in turn filed for government aid on behalf of their unsuspecting users but replaced their bank account where the monies were to be wired. It is reported that between 3,500 to 4,000 aids applications were made fraudulently through this means, amounting to between $34.25 million to $109 million in losses (Cimpanu, 2020).

A global conglomerate is reported to have lost 75% of its mobile devices which was infected by a variant of the Cerberus android banking Trojan attack that compromised the organization's mobile device management server and used it to further to spread the malware (Barth[2], 2020).

The emergence of COVID-19 pandemic has created a rise in theories of the death of cash, and has witnessed the rise in use of crypto currency as well as cybercrimes associated to it, being that crypto currency is often untraceable and has long been associated to conducting transactions on the dark web (Barth, 2020).

Hundreds of thousands of credit card details such as CVV and PIN were reportedly leaked from at least six Southeast Asian countries which include Singapore, Malaysia, Vietnam, Philippines, Thailand, and Indonesia. Among the worst hit was Philippines with a total of 172,828 cards breached, Malaysia 37,145 and Singapore, 25,290 credit card breaches respectively (Sukumaran, 2020).

3.3. Notable Cyberattacks in the 1st Quarter of 2020 (Q1 2020)

Governments and other organizations are taking the initiative to improve on their takedown services, which has paid off by helping to bring down 2,000 online scams related to coronavirus, 471 fake e-commerce platforms, selling fake coronavirus related items, 555 malware distribution sites, 200 phishing sites and busted 832 fraud cases (Palmer[2], 2020). There have been heightened attempts to compromise critical infrastructure, such as hospitals, power stations, petrochemical facilities, pharmaceutical and medical research centers, as well as active deluge of fake news campaign to cause panic, confusion and undermine confidence in political leadership. The lockdown and social distancing order have warranted organizations to reduce their staff levels in enterprise security operation centers while forcing others to work remotely from home, outside enterprise firewalls with vulnerable single-line authentication (Robert, 2020).

It was reported that *Torum,* an English-language dark web internet forum, notably a hotspot for COVID-19 cybercriminal transactions, where a customer was rebuffed by another member for inquiring how best to exploit COVID-19 pandemic, while urging other to show benevolence and avoid taking advantage of an already critical situation (Barth, 2020).

Several governments are using big tech industries to clamp down on dissent views and publications about the pandemic while other countries like China are employing the services of internet police. There are reports that a certain country is deliberately destroying evidence, covering dissent reports on coronavirus by silencing doctors, journalists, activists and scientists who spoke out about the pandemic and criticism of government responses. Their reports were wiped out of the internet with their biography and image deleted, while some of them have gone missing (Markson, 2020). It is imperative that governments and big-tech organizations continue to uphold the right to freedom of expression of its citizen and to support open journalism on this coronavirus pandemic (Ben-Hassine& Dawson 2020).It is imperative for businesses and governments to assist their employees in setting up home-offices digital infrastructure during this lockdown, so as to retain their cyber security standards, especially when it involves the organizations data and confidential information (Meikeng, 2020).

With several governments around the world deploying contact-tracing apps equipped with GPS or Bluetooth technologies, which store all relevant data on a central server. Bluetooth Handshakes between two nearby devices are seen as more private than GPS location tracker but it is not battery efficient meaning users would have to repeatedly re-activate it after engaging with other apps. One of the setbacks, is that Apple does not allow a third-party apps to carry out the process in the background due to security concerns (Cellan-Jones, 2020).

While the battle is ongoing, Google and Apple are co-developing a contact tracing app that matches contacts on individual smartphones, rather than a central server. The proposed app will be designed in such a way that when A meets B, their smart phones exchanges a key code. When A becomes ill with the virus, he updates his status in the app and gives his consent to share his key with the database. B's phone regularly download the database to check for matching codes and will be alerted when someone he/she has been in contact with has tested positive (Cellan-Jones, 2020). The proposed contact tracing app project to be developed by Google and Apple is facing delays as developers are having problems using Bluetooth as means to estimate distance leading to the suspension of the second phase of the project.

Currently, individuals and organizations are experiencing cyberattacks on their personal data, deprived access to their devices and connectivity to the internet but if these attacks are treated with kids glove, it could escalate to a broad-based cyberattack that could cause a widespread digital infrastructure failure that might disrupt activities of a city or a state, especially in the areas of healthcare, networks and public systems (Weforum[2], 2020).

On the other hand, Zoom has issued a statement assuring their subscribers of its optimized security features as well as providing security guidelines and urged users to apply caution about where their zoom videos are saved (Yeoh, 2020). Although Zoom has made video conferencing settings private by default, which warrants users to join the tele-conference using password, certain users continue to set meeting to public for ease of use, which makes it easy for intruders to join the conference, add pornographic links or load malicious software (Malaymail, 2020).

According to Info security, 'there is a 278% rise in leaked government records during Q1 of 2020' totaling 17 million files, as compared to the first quarter of 2019. The first quarter of 2020 has recorded a huge rise in the number of breached records of individuals, politicians, organizations, and governments. A total of 6.9 million organ donor's data was reported lost by the Dutch government, 6.5 million Israeli citizens voter's data was leaked online, while 360,000 teacher's data was exposed in Quebec, Canada (Coker, 2020).

Cyberattacks have increased along with the rapid world wild spread of Covid-19 pandemic. The first quarter of 2020 witnessed an increase of cyber fraud and abuse by 20% resulting in about 445 million attacks reported, of whom most of them revolved round COVID-19. The month of March 2020 witnessed a 650% rise in COVID-19 related email scams. Ransomware attacks against Energy/Utilities service providers witnessed a 32% increase in the first three months of 2020 (Crane, 2020).

S/N	Name of Attack/Victim	Industry	Number of Breaches	Cost
1	Tokopedia	e-commerce	91 million	$5,000
2	Aptoide	Technology	20 million	
3	Zoom	Technology	530,000+	$0.0020
4	A-Lister law firm	Law	756GB	$42 Million
5	BEC (Business Email Compromise) attack	Government		$4 million
6	BEC Scam (Business Email Compromise)	Real estate		$388.700.11
7	Coronavirus-Themed Scam	American Citizens	36,238 (Between Jan1-May 5th, 2020)	$24.44 million
8	SinaWeibo	Technology	538 million accounts	$250
9	Ransomware attack	Government		$7 million
10	easyJet	Aviation	9 million	Yet unknown
11	Minted	Arts	5 million	$2,500
12	homeChef	e-commerce	8 million	$2,500
13	Bhinneka	e-commerce	1.2 million	$1,200
14	Zoosk	Technology	30 million	$500
15	Styleshare	e-commerce	6 million	$2,700
16	ChatBooks	Technology	15 million	$3,500
17	Ggumim	technology	2 million	$1,300
18	Mindful	Health	2 million	$1,300
19	StarTribune	Multimedia	1 million	$1,100
20	The Chronicles of Higher Education	Multimedia	3 million	$1,500

Table 1: Cybersecurity Breaches in Q1 2020
Source: Crane (2020) &Abrams[1] (2020)

4. Findings/Discussions

Cyberattacks are nothing new as it has been occurring since the advent of internet but since the emergence of Covid-19, cyber criminals are cashing in on the situation to inflict more pain on already hurting individuals and businesses by directing attacks against them. In view of the forgoing, certain governments are capitalizing on the situation to advance their surveillance on its citizens and espionage on some of its counterparts. Cyber breaches on web application which recorded 43%, were more than double in the first quarter (Q1) of this year 2020, as compared with the previous year. 86% of breaches were financially motivated while 25% were motivated by espionage (Verizon, 2020).

With losses associated with cyberattacks, businesses and cooperation's are turning towards cyber-insurance, which is rapidly growing with estimated global sales of 7.5 billion Dollars by 2020 (Coventry & Branley, 2018).

Scammers are impersonating Governments, NGO's, cooperation's, and international organizations amongst whom, is the WHO which has witnessed a fivefold increase in cyberattacks since the beginning of Covid-19 pandemic, as compared to the same period in 2019. WHO in a statement claimed they are working with the private sector to establish more robust internal security systems and strengthen their cyber security systems. They are also educating staff of cyber security risks, modus operandi of cyber criminals and are collaborating with big tech organizations and cyber security companies to sanitize our cyberspace (WHO, 2020).

4.1. Findings

The sudden migration of business activities to digital infrastructure necessitated by COVID-19 pandemic, which forced people to work from home has triggered an unprecedented increase in cyberattacks on organizations, businesses as well as individuals. With businesses and government staff working from home, their enterprise standard cyber security is compromised, and cyber criminals are taking the advantage to advance their nefarious acts. Big tech organizations such as Facebook, YouTube and Google are banning and deleting what they regard as descent views about coronavirus pandemic, which left unchecked, might be used as a tool in the hands of oppressive governments. This egregious censorship effort by big tech companies on fact-based science and opinion they consider not in perfect sync with the WHO regulations or guidelines is regarded as misleading, blocked and eventually deleted but studies have shown the WHO is not infallible. This study reveals the following:

- There are heightened attempts by cyber criminals to compromise critical infrastructure, such as hospitals, power stations, petrochemical facilities, pharmaceutical and medical research centers, to further cause pandemonium.
- Big tech giants such as Facebook, YouTube have ordered all dissenting views to be silenced and deleted, as medical professionals, scientists, researchers, and citizens are sharing critical information online.
- The world is currently fighting not only coronavirus pandemic but infodemics, fake news and unprecedented rise in cybercrimes.

- Several governments are taking advantage of this pandemic to advance their digital surveillance on its citizens and espionage on their counterparts.
- There is increased cooperation amongst governments, agencies, and organizations in the fight against COVID-19 pandemic, fake news, and cybercrimes.
- Certain cybercriminal gangs have pledge to cease their attacks on healthcare facilities, nursing homes and emergency response unites while other ransomware operators promised to offer free decryption services for hospitals, they mistakenly encrypted.

The emergence of coronavirus pandemic which led to lockdown of the economy and international borders as well as mandatory stay at home in this 1st quarter of 2020, triggered a high dependence on digital platforms for official, recreational and social reasons and cybercriminals are harnessing the opportunity to perpetuate their nefarious acts on unsuspecting citizens, business and organizations.

4.2. Discussion/Observation

The coronavirus has affected 213 countries and territories and 2 international conveyance, across the globe, as of 12th July, 2020. As at the date, the world has recorded about 13,030,219 cases, 571,242 deaths and 7,577,532 recoveries (World meter, 2020). The data provided in the table below is subject to change, being that occurrences are not static.

Continents/Territories/Conveyance	Confirmed Cases	Deaths	Total Recoveries	Active Cases
Europe	2,570,985	196,566	1,511,540	862,879
North America	3,995,688	185,804	1,837,700	1,972,184
South America	2,893,624	105,156	1,873,771	914,697
Asia	2,959,505	70,286	2,046,345	842,874
Africa	598,236	13,285	298,194	286,757
Oceania	11,460	130	9,331	1,999
Diamond Princess	712	13	651	48
MS Zaandam	9	2	-	7
Global	13,030,219	571,242	7,577,532	4,881,445

Table 2: Continental and International Occurrences of COVID-19
Source: World meter (2020)

The above table illustrates the occurrence of COVID-19 in 6 continents/regions and 2 international conveyance. As at the date, 18 countries and territories are completely free of Covid-19 and out of which, 12 had no casualty while 6 recorded certain degrees of casualties. Certain countries and territories were at some time completely free of Covid-19 but subsequently had new incidents. The Coronavirus is transmitted from human-to human through different mediums and spread globally by rapid movement ofhumans, goods, and services across international boundaries.

5. Conclusion and Recommendation

5.1. Conclusion

The emergence of coronavirus pandemic has shifted all the praise to healthcare practitioners and law enforcement agents but no one remembers the network engineers who kept us all connected by working around the clock, nor cybersecurity personnel that ensures the safety of our cyberspace while we work, do our business or socialize from home. Lack of preparedness for pandemics such as this has left the world in this current economic, political, and social nightmare. While the world watches helplessly and hopes for a miracle as this pandemic ravage our society. Politicians, criminals, and big organizations are contributing to create a cyber-storm that will further hurt our economy, supply chain, businesses, and political ecosystem. This coronavirus pandemic has succeeded in isolating us in our homes but thanks to technology and computerization that has kept us connected virtually and granted us the right tools to work from home and interact with our loved ones over the internet. As the world heralds a technology-driven response to COVID-19, governments and big-tech organizations must recognize and respect international human right laws, adopt best international practice and restrict data collection relevant to public health and research purposes, while upholding transparency in tracking and reporting incidents (Ben-Hassine and Dawson, 2020).

As the world prepare to adapt to 'the new norm' necessitated by the pandemic, we have seen a drop in the number of new incidents and death as well as total recovery from several countries and territories across the globe, cyber security breaches has continued to rise exponentially. We have witnessed cyber criminals pledge to cease their attacks on hospitals and allied industries while some who wanted to take advantage of the situation were rebooked by fellow criminal. Cyber security experts, hackers, tech organizations, agencies and governments have risen to the occasion individually and collectively, by stemming the tide to ensure the security of our cyber space, even as we go through our darkest moments of this pandemic.

5.2. Recommendation

Governments, public health sector, big tech organizations, scientists and agencies as a matter of urgency should work together in the fight against the coronavirus pandemic by aggressively curtailing the spread of the virus through

testing, contact-tracing, development of vaccines, improving security of our cyber space and digital platforms by timely detection, blocking of infected digital contents/phishing accounts tracking and persecution of cyber criminals. The public health systems, research institutes, pharmaceutical as well as the technology industries should be properly funded and equipped with the right tools in handling similar occurrences in the nearest future.

All hands must be on deck in the fight against the COVID-19 pandemic and cyber security threats that is ravaging our world today and the researcher has recommended the following:

- There is need for a committed and united effort in combating the pandemic, by halting the spread and developing the vaccine as well as combating the menace of cyber criminals.
- The sanctity of human rights must be respected by all stakeholders especially now that we are experiencing heightened digital surveillance.
- Big-tech companies and governments must allow a level-playing ground and not silence dissenting voices/opinion.
- Coronavirus is not a myth/hoax as some parties claim it to be; hence WHO regulations must be adhered to.
- There is need for united and committed efforts by all stakeholders in educating the public about the pandemic and cyber security threats, only then we can become partners in the fight.
- We must all work together in the prevention, detection, containment, recovery, and remediation of cyber threats.

6. References

i. Abrams, L[1]. (2020). *Hacker group flood dark web with data stolen from 11 companies.* Bleeping Computer, May 9, 2020 Publication. https://www.bleepingcomputer.com/news/security/hacker-group-floods-dark-web-with-data-stolen-from-11-companies/. Accessed 08/06/2020.

ii. Abrams, L[2]. (2020). *Over 500,000 Zoom accounts sold on hacker's forums, the dark web.* Bleeping Computer April 13, 2020 Publication. https://www.bleepingcomputer.com/news/security/over-500-000-zoom-accounts-sold-on-hacker-forums-the-dark-web/. Accessed 02/05/2020.

iii. Abubakar, U., Anene, N., Abba, M. M., Imran, I. A., Umar, A., & Mubarak, U. (2020). Covid-19 Economic Turbulence and Governments Stimulus Package: A Quest for Survival as Global Recession Looms in the 1st Quarter of 2020. The International Journal of Business & Management (theIJBM). Vol 8, Issue 4, 2020. http://www.internationaljournalcorner.com/index.php/theijbm/article/view/152456/106047. Accessed 22/07/2020

iv. Ahmad, T. (2020). *Corona Virus (COVID-19) Pandemic and Work from Home: Challenges of Cybercrimes and Cybersecurity*. *Available at SSRN 3568830*. https://poseidon01.ssrn.com/delivery.php?ID=094105095110064008004086089018105024001033030064027066098109068088068012091004006071020045051127023056111099107028079094115066107001090050083100107095107088105111120036022056002077019084115121096123001018097093114124001072122001023118087029118087125114&EXT=pdf. Accesses 23/04/2020/

v. Anene, N., Abubakar, U., Ogechi, O. P., Abba, M. M., Umar, U., &Maikarfi, R. M. (2020). *Coronavirus and Social Media: A Heuristic Approach in the Face of Pandemic.* International Journal of Science &Technology (IJST)Vol 8 Issue 4. http://52.172.159.94/index.php/theijst/article/view /152399 /106002. Accessed 22/07/2020.

vi. Barth, B[1]. (2020). *5 ways COVID-19 is reshaping the cybercrime economy.* SC Media publication of April 30, 2020. https://www.scmagazine.com/home/security-news/news-archive/coronavirus/5-ways-covid-19-is-reshaping-the-cybercrime-economy/. Accessed 02/05/2020.

vii. Barth, B[2]. (2020). *Banking Trojan attack exposes dangers of not securing MDM solutions.* SC Media publication of May 1, 2020. https://www.scmagazine.com/home/security-news/mobile-security/banking-trojan-attack-exposes-dangers-of-not-securing-mdm-solutions/. Accessed 03/05/2020.

viii. BBC, (2020). *Houseparty offers $1m reward for proof of sabotage.* Published British Broadcasting Corporation March 31, 2020. https://www.bbc.com/news/technology-52101421. Accessed 01/05/2020

ix. Ben-Hassine, W.& Dawson, P. (2020). *4 rules to stop governments misusing COVID-19 tech after the crisis.* World Economic Forum, May 15, 2020 publication. https://www.weforum.org/agenda/2020/05/covid-19-tech-data-usage-privacy/. Accessed 04/06/2020.

x. Cellan-Jones, R. (2020). *Coronavirus:* State surveillance 'a price worth paying'. BBC News, April 24, 2020. https:// www.bbc.com/news/technology-52401763. Accessed 05/05/2020

xi. Cimpanu, C., (2020). *German government might have lost tens of millions of euros in COVID-19 phishing attack.* ZDNet[3], April 18, 2020 publication. https://www.zdnet.com/article/german-government-might-have-lost-tens-of-millions-of-euros-in-covid-19-phishing-attack/. Accessed 25/04/2020

xii. Coker, J. (2020). *278% Rise in Leaked Government Records during Q1 of 2020.* Infosecurity Magazine, April 15, 2020 publication. https://www.infosecurity-magazine.com/news/rise-leaked-government-records/. Accessed 05/06/2020

xiii. Coventry, L.&Branley, D. (2018). *Cybersecurity in healthcare: Anarrative review of trends, threats and ways forward.*https://www.sciencedirect.com/science/article/pii/S0378512218301658?casatoken=OBpnW-PMA6w AA A AA: t5yfIKONULnMHsPAcf3FocsnH2S2MSsgv5XnRF33ma6EowdgxYcGqWEwjIKO8y0-uoP5wgF841zO. Accessed 14-07-2020

xiv. Crane, C. (2020). *The Definitive Cyber Security Statistics Guide for 2020.* Security Boulevard, May 15, 2020 publication. https://securityboulevard.com/2020/05/the-definitive-cyber-security-statistics-guide-for-2020/. Accessed 05/06/2020.

xv. Fiddler, P. (2020). *Cybersecurity in the time of COVID-19*. Council on Foreign Relations, March 30, 2020 publication. https://www.cfr.org/blog/cybersecurity-time-covid-19.Accessed 04/05/2020.

xvi. Hodge, R. (2020). *Zoom security issues: Zoom bombings continue, include racist language and child abuse.* c|net, April 24, publication. https://www.cnet.com/news/zoom-security-issues-zoombombings-continue-include-racist-language-and-child-abuse/. Accessed 27/04/2020.

xvii. Hope, A. (2020). *Cybercrime Gangs Promise to Stop Attacks on Healthcare Organizations During the COVID19 Crises*. CPO Magazine, March 25, 2020 publication. https://www.cpomagazine.com/cyber-security/cybercrime-gangs-promise-to-stop-attacks-on-healthcare-organizations-during-the-covid-19-crisis/. Accessed 24/04/2020.

xviii. Irwin, L. (2020). *List of data breaches and cyber attacks in May 2020 – 8.8 billion records breached.* it governance 1st June, 2020 publication. https://www.itgovernance.co.uk/blog/list-of-data-breaches-cyber-attacks-may-2020.Accessed 12/06/2020.

xix. KPMG, (2020). *Get ahead of cyber security breaches.* KPMG 2020 Publication. https://home.kpmg/xx/en/home /insights/2019/05/get-ahead-of-cyber-security-breaches.html. Accessed 12/06/2020.

xx. Lawrie, E. (2020). *Coronavirus: How does contact tracing work and is my data safe*. BBC News, April 30, publication.https://www.bbc.com/news/explainers-52442754?intlink_from_url=https://www.bbc.com/news/technology&linkloc ation =live-reporting-story. Accessed 01/05/2020.

xxi. Lyengar& Fung (2020). *Zoom, the video conferencing app everyone is using, facing questions over privacy.* CNN Business, April 1, 2020 publication. https://amp.cnn.com/cnn/2020/04/01/tech/zoom-video-privacy-concerns/index. html?_twitter_impression=true Accessed 28/04/2020.

xxii. Malaymail, (2020). *Singapore MOE suspends use of Zoom for home-based learning after hackers hijack classes. Malaysia's* MalayMail Newspaper Publication of 10th April, 2020. https://www.malaymail.com/amp/news/tech-gadgets/2020/04/10/singapore-moe-suspends-use-of-zoom-for-home-based-learning-after-hackers-hi/1855338? Utmterm=Autofeed&utm_medium=Social&utm_source=Twitter&__twitter_impression=true.Accessed 27/04/2020.

xxiii. Markson, S. (2020). *Coronavirus NSW: Dossier lays out case against China bat virus program.* The Daily Telegraph, May 4, 2020 publication. https://www.dailytelegraph.com.au/coronavirus/bombshell-dossier-lays-out-case-against-chinese-bat-virus-program/news-story/55add857058731c9c71c0e96ad17da60. Accessed 07/05/2020

xxiv. Mauro, A. (2020). *Working from home during the coronavirus pandemic creates new cybersecurity threats.* The Conversation, April 9, 2020 publication. https://theconversation.com/working-from-home-during-the-coronavirus-pandemic-creates-new-cybersecurity-threats-134954. Accessed 02/05/2020.

xxv. Meikeng, Y. (2020). *Cybersecurity cases rises by 82.5%.* The Star, April 12, 2020 publication. https://www.thestar.com.my/news/focus/2020/04/12/cybersecurity-cases-rise-by-825. Accessed 05/05/2020.

xxvi. Palmer, D. (2020). 2,000 *coronavirus scammers taken offline in major phishing crackdown.* ZDNet2, April 21, 2020. https://www.zdnet.com/article/2000-coronavirus-scammers-taken-offline-in-major-phishing-crackdown/. Accessed 25/04/2020

xxvii. Palmer, D. (2020). Coronavirus scams: this is how much people have lost online to fraudsters so far. ZDNet1, April 17, 2020. https://www.zdnet.com/article/coronavirus-scams-this-is-how-much-people-have-lost-to-online-fraudsters-so-far/. Accessed 25/04/2020

xxviii. Platta, S. (2020). *Hackers just leaked sensitive files from over 200 police departments that are searchable by badge numbers.* Yahoo news, June 22, 2020 publication. https://news.yahoo.com/hackers-just-leaked-sensitive-files-154620446.html. Accessed 28/06/2020

xxix. Robert, R., A., Jr. (2020). *The Coronavirus & Cybersecurity: 3Areas of Exploitation.* Dark Reading April 7, 2020 publication. https://www.darkreading.com/the-coronavirus-and-cybersecurity-3-areas-of-exploitation-/a/d-id/1337465. Accessed 03/05/2020.

xxx. Sukumaran, T. (2020). *Singapore, Malaysia credit card details dumped online in massive data breach.* Asiaone, March 7, 2020 publication. https://www.asiaone.com/singapore/singapore-malaysia-credit-card-details-dumped-online-massive-data-breach. Accessed 07/05/2020.

xxxi. Tidy, J. (2020). *Coronavirus: Facebook alters virus action after damning misinformation report.* BBC News, April 16, 2020 publication. https://www.bbc.com/news/technology-52309094. Accessed 25/04/2020.

xxxii. Tung, L. (2020). *Google to Gmail users: Coronavirus phishing is targeting you. This is how we hit back. ZDNet4* April 16, 2020 publication. https://www.zdnet.com/article/google-to-gmail-users-coronavirus-phishing-is-targeting-you-this-is-how-we-hit-back/. Accessed on 28/04/2020

xxxiii. Umeh, J. (2020). *Cyber security: How attackers impersonate WHO, on COVID-19.* Vanguard newspaper, April 1, 2020 Publication. https://www.vanguardngr.com/2020/04/cyber-security-how-attackers-impersonate-who-

on-covid-19/amp/?utm_source=dlvr.it&utm_medium=twitter&__twitter_impression=true. Accessed on 24/04/2020.

xxxiv. UN, (2020).UN tackles 'infodemic' of misinformation and cybercrime in COVID-19 crisis. https://www.un.org/en/un-coronavirus-communications-team/un-tackling-%E2%80%98infodemic%E2%80%99-misinformation-and-cybercrime-covid-19. Accessed 23/04/2020

xxxv. Verizon, (2020). *2020 Data Breach Investigation Report.* Verizon 2020, Publication. https://enterprise.verizon .com/en-gb/resources/reports/dbir/. Accessed 05-072020.

xxxvi. Weforum[1], (2020). *Why COVID-19 makes the case to get rid of passwords*. April 1, 2020 publication of World Economic Forum. https://www.weforum.org/agenda/2020/04/covid-19-is-a-reminder-that-its-time-to-get-rid-of-passwords. Accessed on 23/04/2020.

xxxvii. Weforum[2], (2020). *Why cybersecurity matters more than ever during the corona virus pandemic*. March 17, 2020 publication of World Economic Forum. https://www.weforum.org/agenda/2020/03/coronavirus-pandemic-cybersecurity/. Accessed 23/04/2020.

xxxviii. WHO, (2020), *Beware of criminals pretending to be WHO.* World Health Organisation.https://www.who.int/ about/communications/cyber-security. Accessed 23/04/2020

xxxix. WHO[2], (2020). *WHO reports fivefold increase in cyberattacks, urges vigilance.* World Health Organisation. https:// www.who.int/news-room/detail/23-04-2020-who-reports-fivefold-increase-in-cyber-attacks-urges-vigilance. Accessed 22/07/2020.

xl. Worldometer, (2020). *Covid-19 Coronavirus Pandemic*. https://www.worldometers.info/coronavirus/. Accesses 12/07/2020.

xli. Yeoh, A. (2020). *Thousands of private Zoom video recordings exposed online.* TheStar, April 6, 2020 publication. https://www.thestar.com.my/tech/tech-news/2020/04/06/thousands-of-private-zoom-video-recordings-exposed-online. Accessed 27/04/2020.

xlii. Zolkeple, F. (2020). 556 cases of face mask scams so far, RM4.2mil lost. TheStar Newspaper[1], April 4, 2020 publication. https://www.thestar.com.my/news/nation/2020/04/04/556-cases-of-face-mask-scams-so-far-rm42mil-lost#cxrecs. Accessed 25\04\2020