International Journal of Advance and Applied Research
www.ijaar.co.in
ISSN – 2347-7075 Impact Factor – 7.328
Peer Reviewed Bi-Monthly
Vol. 11 No. 4 March-April 2024

Covid 19 Impacts on Cyber Security: Issues and Challenges

Syamsundar Reddy[1], G Anjan Babu[2]
[1]Research Scholar, Department of Computer Science, SVU College of Commerce, Management & Computer science, Sri Venkateswara University, Tirupati
[2] Professor, Dept. Of Computer science, SVU College of Commerce, Management & Computer Science, Sri Venkateswara University, Tirupati
Corresponding Author – Syamsundar Reddy
Email: cssreddi@gmail.com
DOI- 10.5281/zenodo.11057744

Abstract:
Although cyber technologies benefit our society, there are also some related cyber security risks. For example, cybercriminals may exploit vulnerabilities in people, processes, and technologies during trying times, such as the ongoing COVID-19 pandemic, to identify opportunities that target vulnerable individuals, organizations (e.g., medical facilities), and systems. In this paper, we examine the various cyber threats associated with the COVID-19 pandemic. We also determine the attack vectors and surfaces of cyber threats. Finally, we will discuss and analyze the insights and suggestions generated by different cyber attacks against individuals, organizations, and systems.

Keywords: COVID-19, Cyber Threat, landscape, Opportunities and challenges

Introduction:

It is unbelievable how global events turned out so dramatically in 2020, particularly how the cyberspace became disrupted, not by a devastating atomic bomb or a trans-ocean teletsunami but by a mere biological virus whose infinitesimal diameter is estimated to be only approximately 125 nanometers, or equivalent to 600 times smaller than the diameter of the human hair; that is the novel coronavirus, pathogen that ignited the pandemic, the game changer. 2020 plans and budgets were disrupted [1], everyday life was impacted [2], and the world came to a standstill as authorities compelled people to stay at and work from home (WFH), even using coercion [3] to enforce the lockdown. There were no year 2020 predictions that came close to the magnitude of devastation caused by the outbreak of the coronavirus disease that was later renamed COVID-19 and classified as a pandemic by the World Health Organization. The statistics are increasing at the time of this research. For example, according to the data provided by the World Health Organization (WHO), more than 4.5 million new cases were reported in the week of April 5, 2021, and the number of new deaths increased for the fourth consecutive week, an increase of 7% with more than 76,000 new deaths reported.2 In response, governments have introduced measures such as lockdowns, quarantines, remote work, distance learning, social distancing, and travel bans[2]. Cybercriminals find the uncertainty brought by changing daily habits opportune and the increased virtual existence is converted into available attack vectors. According to data from the Federal Bureau of Investigation (FBI), it is reported that during the pandemic, cybercrime increased by 400%.Interpol has also reported that during the COVID-19 pandemic, cybercrimes increased.[3]

Identified Cyber Security Challenges During Pandemic:

Challenges with the Technical Security

Various IT-related challenges surfaced throughout the teleporting period. The county had many IT tools in place but lacked the means to create a secure teleporting environment. Alpha expressed concerns regarding which tools are deemed secure to use in which situations while the county had not yet had resources to assess all the risks associated with the IT environment. For example, Alpha was using all or some of the same meeting platforms available within the whole county; Skype for Business, Teams, Cisco VMR (Virtual Meeting Room), Zoom, and Cisco Video Conferencing. The work routines dictated them to choose from a pool of various communication tools since various authorities and organizations within the county use different tools. The challenge for Alpha was to answer users' (i.e., other employees within the county) questions regarding the security of different tools and platforms since the tools´ assessments have either not been widely known within the county or simply have not been completed.

Challenges with the Policies and Regulations

This challenge relates to the rules and regulations in place regarding information security when teleporting within the county. In general, it

was observed that the employees had not spent any time before the focus group session to reflect on the rules for teleporting. This finding came as a surprise because cyber attacks have been a hot topic within the county during the pandemic. The situation could be related to the fact that no rules or regulations regarding information security when teleporting could be found on the county´s intranet or that the information was not accessible to all. Instead, employees are expected to act with common sense and adapt their security behavior from in-office to teleporting. This might be a reasonable expectation of employees at Alpha owing to their technical competencies. However, in the broader perspective, this is not sufficient for employees that do not work with information security or questions related to information security. Participants from the focus groups believed that this situation needs to be improved and demanded:

Challenges with the Information Security Awareness

As part of their tasks prior to the pandemic, Alpha had previously worked continuously to raise employees' awareness regarding information and IT security practices to safeguard the information. However, broadening that awareness to be applied while teleporting has not been a focus. Internally, Alpha has discussed issues related to teleworking from various perspectives, such as IT security and information security. However, they have not identified similar discussions being held in a significant number of Alpha's departments within the county. The responsibility of ensuring that employees follow regulations and policies regarding information security lies with the individual department managers, and they are tasked with following up that their employees follow the established regulations. However, no follow-ups have been made in connecting to the increase of teleworking.

Challenges with the Preparedness

This theme deals with the level of preparedness on information security and teleporting before the pandemic and the continued preparedness for potential issues after the pandemic.

An example of the issues Alpha experienced was that the VPN was not dimensioned for the increased number of users and forced the IT department to quickly upgrade and divide the users into different connections. If the county did not have the tools and culture for teleporting, issues like the VPN might not have been surprising. However, considering the efforts towards digitalization and the much collaboration within Sweden and internationally, this was unexpected.[4]

Fields/ dept. affected by cyber threats during pandemic

Cybercriminals have identified COVID-19 disinformation as an opportunity to target research, healthcare organizations, government agencies and financial institutions (FIs) with the knowledge that these organizations are focusing on the pandemic (PwC 2020; WEF 2020; WHO 2020a). Threat actors know that it might take some time before their nefarious acts are discovered because considerable attention is spent on mitigating the COVID-19 pandemic. The following discussion focuses on financial services, healthcare organizations and government agencies as prime targets for cybercrimes during the COVID-19 pandemic.

Financial services During the COVID-19 pandemic, global systems have been attacked and millions of United States dollars have been lost through cybercrimes. Stock markets around the world and every aspect of the economy have been severely affected. The financial services industry has been attacked through phishing, malware and ransom ware (Khan et al. 2020). With reference to widespread incidents of cyber attacks and threats, South African banks have embarked on a drive to educate their clientele regarding fake emails and phishing (South African Banks Risk Information Centre [SABRIC] 2020). A wide range of phishing scams (i.e. bogus communications that purport to be from a well-known and trusted source, which request confidential information [typically login/password details or banking information]) are circulated by hackers.

Healthcare systems most healthcare organizations rely on ICT applications, which offer patients and healthcare personnel e-healthcare services. The COVID-19 pandemic has exposed these e-healthcare services, escalating the battle currently faced by healthcare institutions resulting in overstretched resources and personnel that are responding to the novel corona virus (Khan et al. 2020). In the United States, the CDC and other healthcare facilities have been attacked by Dodos through millions of connection requests. The WHO was also exposed to malicious attacks thrown at a critical time for global response and a key component of a collective resilience. The attack on the WHO impacted critical services where criminals launched spear-phishing attacks imitating the WHO and CDC, using the pandemic to spread malware and ransom ware and launch fraudulent websites to prey on users (Balsom & Dixon 2020).

Government and other outlets At a time when South Africa's Parliament is closed and all its meetings are currently held by video conference calls as the country remains under strict lockdown regulations, hackers disrupted the meeting by sharing obscene material using the Zoom platform during the virtual held meeting (Ogomotsi Magome 2020). In addition to the rapid growth of Zoom's popularity being deemed as unsafe in many countries, it has been banned in United States and Taiwan for communication (Khan et al. 2020).

South African institutions are staying in touch with their clients and employees through Microsoft Teams, Google Meet and Zoom, despite cyber threats and hacking incidents on Zoom meetings.[5]

Although patients were not affected, district employees used their systems and network to exchange information regarding the Corona virus outbreak. While the attack was being investigated, the health district turned to face book to share information among themselves and with the public. However, this solution has its own risks, since anyone can falsify their identity on social media and attempt to breach the organization.[6]

Major authoritative issued many warnings to the public about cybercriminals aiming to take advantage of people in these difficult times. These warnings highlight that criminals are setting up fake Web domains to disguise themselves as the WHO. According to WHO, more than 4000 Corona virus-related domains have been registered since the beginning of the year, 5% of which are viewed as suspicious and 3% of which are new domains that are considered malicious.[7]

Figure-1 – covid-19 Impact on cyber security.

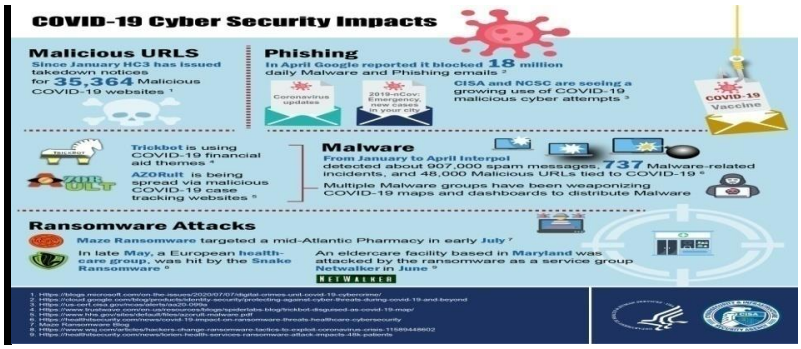

Figure-1 – covid-19 Impact on cyber security

Major Incidents Noticed In Pandemic:

During the early months of COVID-19, numerous studies reported on the negative impacts and stressful events associated with the first series of global lockdowns. Here, we distinguish between psychological experiences during COVID-19 (e.g., feeling stressed, sad, or lonely) and COVID-19 stressful events (e.g., job loss, death). Heightened levels of mental health difficulties were commonly reported (e.g., distress, anxiety, depression). However, emerging longitudinal research suggests these effects may be small, and there is likely considerable variability in the psychological experiences of COVID-19. Nevertheless, psychological harms, concern towards the health of vulnerable loved ones, as well as loss of leisure and health activities, were commonly reported during the early months of COVID-19. In the first few weeks of the pandemic; these were among a number of studies to report that COVID-19 exacerbated the struggles of groups experiencing various difficulties prior to the onset of the pandemic. In another early pandemic study, Ibo and colleagues found that COVID-19 instigated an amplification of pre-existing inequalities among disadvantaged groups including ethnic minority groups, those experiencing socioeconomic disadvantages, and the unemployed. Furthermore, in a qualitative study of distress and coping in India during the first COVID-19 lockdown, disadvantaged groups with limited access to mobile phones, health messaging, or health care experienced extreme distress and despair, greater health needs, loss of income, and further social exclusion as a result of the pandemic. Social isolation has been commonly reported as a primary cause of increased psychological distress among some individuals during COVID-19. students revealed that individuals without pre-existing mental health concerns were more likely than individuals with pre-existing mental health concerns to experience declining mental health during the early months of the pandemic, which corresponded with increased social isolation among these students (whereas there was no change for students with pre-existing mental health concerns). Other contextual factors that have been found to be contributors to negative COVID-19 experiences among general population samples during the early months of the pandemic include economic fallout (e.g., wage loss), grief from having lost a loved one to COVID-19, trauma associated with surviving COVID-19, the inability to see relatives (especially older relatives), having to manage the impracticalities of working or schooling from home, the disruption of social and recreational activities, and frustration with the media or government] In short, much of the literature has focused on the negative consequences associated with COVID-19 events without accounting for the possibility of positive experiences emanating from COVID-19 events.[7]

Financial Losses And Infrastructure Losses:

The global trade finance gap is estimated at $1.7 trillion in 2020, having increased 15% from the latest estimate of $1.5 trillion in 2018 (Figure 1). As a percentage of global goods trade, the gap increased to 10% in 2020 from 8% in 2018. Firms'

demand for trade finance declined as the COVID-19 pandemic dampened world trade and disrupted global value chains. However, the likelihood of trade finance applications being rejected rose significantly as the pandemic heightened economic and financial uncertainties while trade- and finance-related transactions costs increased because of supply disruptions. As the availability of trade finance is essential to trade, its shortage could have contributed to the global trade contraction during the pandemic. Despite the widened trade finance gap, the responses from banks indicate that 79% of them did not reduce capital availability and 73% of them did not reduce limits to support trade during the pandemic.[8]

The Organization for Economic Co-operation and Development (2020) reports that the initial quarter of 2020 saw the lowest GDP growth for the G20 since data have been kept in 1998 at -3.4%. The decline escalated to -6.9% in the 2nd quarter of 2020, demonstrating that the damage to the economy was greater than the -1.5% hit during the global recession of 2008 In the first quarter of 2020, the United States saw a shock of -1.3%, which dropped to -9.1% in the 2nd quarter; the United Kingdom saw decreases of -2.2% and -20.4%; and France of -5.9% and -13.8. In Asia, India saw a 0.7% first-quarter shock and a -25.2% second-quarter shock; Korea experienced a 1.3% and a -3.2% shock; Japan experienced a 0.6% and a 7.9% shock; and China experienced a 10.0% and 11.5%. The International Monetary Fund (2020) forecast a -4.4% yearly rate of growth for the world in 2020 based on the outbreak and related restrictions measures. 2020 saw only China's significant economy expand. A 2.3% increase was recorded. On the other hand, the IMF expects a 5.2% world economy in 2021. China and India, which are predicted to grow, correspondingly, will be the main drivers of that. In major, highly reliant on resources countries that have been severely harmed by the crisis, recovery is predicted to be protracted.[9]

Mitigation Steps Taken:

It is important to keep in mind what economic policy can and cannot do. The objective is not and cannot be to eliminate the recession altogether. The recession will be there, it will be massive, but hopefully short-lived. Instead, the priority is to short-circuit all the negative feedback loops and channels of contagion that otherwise amplify this negative shock. Unchecked, the recession threatens to destroy the complex network of economic linkages that allows the economy to operate and would take time to repair. To ensure that workers can remain employed – and collect their wages – even if quarantined or forced to stay home to look after dependents. Temporary layoff assistance is a key component; without it, it is even unclear whether public health advisories can be followed. Households need to be able to make basic payments (rent, utilities, and mortgages, insurance). 2. To ensure that firms can weather the storm without going into bankruptcy, with easier borrowing terms, possibly temporarily waving tax or payroll payments, suspending loan payments, or providing direct financial assistance where needed. 3. To support the financial system as non-performing loans will mount, so as to ensure the crisis does not morph into a financial crisis.

Cyber Security threats: -

Financial institutions are always favorite among cyber criminals. During this difficult time with the increasing needs of remote working and more uses of digital approach by banks and their customers, there is a growing concern for cybercrimes. It has been observed that now days malware attacks have becoming more and more frequent. The banking frauds in India have increased during this pandemic situation.

Table 1: Cyber Security Threats

Bankgroups/ Institution	Number Of Frauds
Public sector banks	2,903 (39.0)
Private sector banks	3710 (59.4)
Foreign banks	521 (7.1)
Financial institutions	25 (0.3)
Small finace banks	114 (1.6)
Payments banks	88 (1.2)
Local area banks	2.00 (0.0)
Total	7363 (100.0)

Source: RBI, 2021b

According to RBI's annual report for 2019-20, the amount involved in banking frauds has higher in private sector banks compare with other banking institutions. If there is a privacy breach or breach in security in a bank, it basically leads to the information of the customers being sold or purchased on the dark web by other cybercriminals. Ultimately these types of privacy breach led to loss of data and earnings for a banking institution, disruptions in their operations, loss of reputation of that bank along with loss of their both actual and potential customers. [11]

Solutions:

Given the events of the past year, it is imperative to integrate state-of the-art solutions into the lives of users worldwide. We want to encourage users, casual and professional alike, to consider these solutions to not only prevent cyber at tacks, but to also be prepared in the event of an incident. The potential solutions to these cyber attacks can be categorized as countermeasures to cyber threats or privacy enhancements. These solutions will not only help users prevent and mitigate attacks, but will also inform them of the risks at hand and allow preemptive preparation for any incidents, both at home and in the workplace. According to Dark Matter's cyber security report and the warnings published by WHO Interpol, and Kasper sky, the following are general recommendations for countermeasures against cyber attacks based on the analysis of cyber security vulnerabilities of key infrastructures previously attacked. In addition to organizations taking extra precautions and becoming more aware of cyber risks, law enforcement authorities must also be prepared to handle cyber attacks. Typically, law enforcement officers have departments that handle cyber security-related issues. However, due to the increased network activity occurring during quarantine, these departments may become short-handed, and traditional officers may need to step in to assist. As stated by WHO, Interpol, and Digit poll, hotlines have opened up for people to call or write tickets to report any scam attempts or cyber attacks. Given the increase in cyber attacks worldwide, these organizations need to be prepared and familiar with cyber security.[12]

Recommendations:

While conducting the research, some limitations are reported here. Firstly, cyber security and the COVID-19 outbreak are dynamic in nature; they can change on a day-to-day basis, they have the ability to rapidly evolve, and they are unpredictable to an extent. Although the material included in this paper is as recent as possible, the information shared may change after some time. This entails a close and sustained follow-up to new issues related to cyber security and COVID-19. The cyber attacks that were covered in the previous Sections are very relevant to the time of this work. However, hackers are always actively attempting to compromise and take advantage of people and organizations, and their methods of doing so may evolve. This is how cyber security can be unpredictable; specialists can prepare for known cyber attacks and resolve known flaws and vulnerabilities, but they cannot foresee evolving versions of cyber attacks. In other words, cyber security specialists cannot foresee zero-day attacks, hence the name "zero-day." The unpredictability of cyber security is also the result of the inability to predict a nation's next move. Earlier in this paper, several cyber attack attempts by Iran and other nations were mentioned. The plans to pull off these attacks are considered privileged knowledge, and only those involved in the attack know these plans. The most that people and organizations can do is to preemptively protect themselves from known behaviors and attacks. On the other hand, this is a sincere call to share knowledge and experiences globally to deal with cyber security threats and COVID-19. Another limitation when studying the materials in this paper is the limited availability of information. To the best of our knowledge, most of the materials covered in this paper came from a variety of resources. Nevertheless, information regarding cyber attacks on organizations and critical infrastructures during this pandemic is very limited; there are articles about the attack occurring, but many of the details about the attack remain confidential. In addition to our previous recommendation of sharing experiences globally, there is a great push to research cyber security and COVID-19, and the coming weeks and months will witness a great growth in published material in this direction. To reduce the number of cyber attacks during such difficult times and in the future, governments can inform their country's residents of cyber safety practices with the announcement of the home quarantine. Early awareness can let users understand the dangers of excessive Internet activity and how cybercriminals will attempt to harm their systems. Users should be encouraged not to share personal information immediately and to doubt the source of a message or email. Policy makers, educators and legislators should play a major role here in developing (and coaching) enforcing policies, procedures and guidelines to govern both cyber security and COVID-19 threats in order to surround the crisis and prevent chaotic situations. Developers of web applications, such as Zoom or the interactive COVID-19 maps should make sure that software development lifecycle. Personal accounts. People need to avoid sharing personal information or opening suspicious web pages and applications. This study attempts to include the latest literature to shed light on the dangers of cyber security in the ongoing COVID-19 pandemic, while raising important

alarms. This is an emerging and a growing phenomenon and a global threat. This requires the cooperation and collaboration of different global stakeholders to control COVID-19 and hence, limit and stop the growth of cyber security threats. The research provided different recommendations and implications for both professionals and researchers, paving the way for more research in this crucial area.

Conclusion:

The COVID-19 pandemic has generated remarkable and unique societal and economic circumstances leveraged by cyber-criminals. Our analysis of events such as announcements and media stories has shown what appears to be a loose correlation between the announcement and a corresponding cyber-attack campaign which utilises the event as a hook thereby increasing the likelihood of success. The COVID-19 pandemic, and the increased rate of cyber-attacks it has invoked have wider implications, which stretch beyond the targets of such attacks. Changes to working practices and socialization, mean people are now spending increased periods of time online. In addition to this, rates of unemployment have also increased, meaning more people are sitting at home online- it is likely that some of these people will turn to cyber-crime to support themselves. The combination of increased levels of cyber-attacks and cyber-crime means there may be implications for policing around the World law enforcement must ensure it has the capacity to deal with cyber-crime.

References:

1. Kenneth Okereafor -"Cyber security in the COVID-19 Pandemic", March 2021,pg1 to 2 DOI:10.1201/9781003104124, ISBN: 9781003104124
2. C. Sohrabi, Z. Alsafi, N. O'Neill, M. Khan, A. Kerwan, A. Al-Jabir, C. Iosifidis, R. Agha, World health organization declares global emergency: a review of the 2019 novel coronavirus (covid-19), Int. J. 76 71–76.
3. S. AlDaajeh, H. Saleous, S. Alrabaee, E. Barka, F. Breitinger, K.-K.R. Choo, The Role of National Cyber security Strategies on the Improvement of Cyber security Education, Computers & Security, 2022, 102754.
4. Ali padab –"Challenges of Managing Information Security during the Pandemic", Published: 16 November 2021, https://doi.org/10.3390/challe12020030
5. Joel Chigada, Rujeko Madzinga-Cyberattacks and threats during COVID-19: A systematic literature review, South African Journal of Information Management ISSN: (Online) 1560-683X, (Print) 2078-1865, Pg NO.4-5, 2021.
6. D. Pressey, C-u public health district's website held hostage by ransom ware attack, The News-Gazette[Online]. Available: https://www.news-gazette.com/news/l ocal/health-care/c-u-public-health-district-s-website-held-hostage-by/article_2d adedcd-aadb-5cb1-8740-8bd9e8800e27.html.
7. https://www.ncbi.nlm.nih.gov/pmc/articles/PM C9231712/University of Virginia, Fake corona virus map delivers azorult malware, Information Security at UVA [Online]. Available: https://security.virginia.edu/fake-corona virus-map.
8. Kijin Kim -2021 Trade Finance Gaps, Growth, and Jobs Survey, Economist Asian Development Bank, pg.no. 192, OCTOBER 2021.
9. Sethi, Rajiv -Impact of COVID 19 on Global Economy with Special Reference to India, pg.7, 2023.
10. Richard Baldwin and Beatrice Weder di Mauro –"Mitigating the COVID Economic Crisis: Act Fast and Do Whatever It Takes", pg-36, A VoxEU.org Book.
11. Digitpol, Covid-19 cyber attack investigation [Online]. Available: https://digitpol.c ohm/covid-19-cyber-attack-investigation/
12. Heba Saleous a, Muhusina Ismail a "COVID-19 pandemic and the cyber threat landscape: Research challenges and opportunities" Digital Communications and Networks 9 (2023) 211–222.