Impact of COVID-19 on Cyber Space

Sr .Jainy Jacob M
Mercy College Palakkad, Kerala,India

Abstract

The pandemic dependence on digital technologies and bolsters for scourge and cyber espionage. Public health measures, other equally interments, produced a surge in online activities. The ability of technical school corporations and also the web to handle the demand underscored the outstanding capabilities that Net provides. However, this crisis-induced dependence created an even more fertile field for cybercrime and cyber espionage, which, even before the pandemic, constituted serious threats. Pandemic-related incidents , such as criminal ransom ware attacks on healthcare and cyber espionage against vaccinations , the most attention , but the online surge increased the incentives for and intelligence agencies to use cyber vulnerabilities all told sectors of economic and political activity. This article examines the impact of COVID-19 on cyber risk and mitigation measures that businesses can take.

INDEXED TERMS :- CYBER SPACE, CYBER-ATTACK ,CYBER SECURITY, **DENIAL OF SERVICE (DOS) ATTACK,** PHISHING, MALWARE, **RANSOM WARE ATTACKS**

INTRODUCTION

Humanity has been full of many diseases and epidemics since the first days. However, the quantity and prevalence of those diseases haven't redoubled dramatically over the past decades, as happening recently. This noticeable shift in recent times is that the results of multiple factors wherever earth science and widespread trade can be one in every of the explanations in pandemic unfold.2020 will be remembered as a singularly disturbing year, but not just as a global health crisis. Life online has undergone a digital transformation as exponential changes at work from home and through cyberspace are accelerating. With the explosion of security incidents and cyber incidents changing society in many ways, this year will also be remembered as in 2020.The coronavirus pandemic has created new challenges for businesses as they adapt to associate in operation model within which acting from home has become the 'new normal'. firms square measure fast their digital transformation, and cyber security is currently a serious concern. The reputational, operational, legal and compliance implications may well be substantial if cyber security risks square measure neglected. Cyber security at the time of COVID-19 is additionally thought of anotherpandemic wherever several attacks area unit launched during a} very short time. though this pandemic and also the whole world area unit busy sorting out a cure, cyber security crimes had been increased lately.

A. Impact of COVID-19 on digital working and cyber security

The restrictions imposed by governments in response to the coronavirus pandemic have encouraged employees to work from home, and even 'stay at home'. As a consequence, technology has become even more important in both our working and personal lives. Despite this rise of technology need, it is noticeable that many organizations still do not provide a 'cyber-safe' remote-working environment. Where business meetings have traditionally been held in-person, most now take place virtually.

In June 2020, Swissinfo.ch reported data from the NCSC (National Center for Cyber Security) showing that in April, Switzerland reported 350 cyber attacks (phishing, fraudulent websites, direct attacks on companies, etc.), compared to 100- 150. The coronavirus pandemic and the increase in working from home are considered the main reasons for this increase, as people who work from home are not able to enjoy the same level of inherent protection / deterrence measures (such as internet security) of the environment labor.

Defining a cyber-pandemic is a bit like defining a "perfect storm", except that this storm occurs in cyberspace. There are many active sections, including the "all of the above" list of threats and cyber-attacks listed in items 1-7 in figure 1 below. From ransom ware to data breaches, from election security to unemployment fraud, COVID-19 has triggered new challenges and/or accelerated existing challenges in global business in many ways. It is obvious that technology and security professionals will strive to respond to the changing environment as quickly as bad actors in 2020, taking advantage of unprecedented changes in people, processes, and technology wise.

The pandemic poses a great challenge for global companies: Despite the massive closure of offices and other facilities, they must continue to function. Information technology they have long relied on (data centers, cloud systems, departmental servers, and the digital devices used by departing employees to stay connected to each other and to stay in touch with Data Company) has become more important. . Overnight, the demand for digital infrastructure skyrocketed. Technologies like have also become bigger and more profitable targets for cybercriminals. Cyber security needs to be updated to avoid a second crisis: in digital devices and networks that have been critical to the business in recent weeks. In other words, "business continuity" has become a mandatory requirement.

Here are the different kinds of pandemic-related scams that took place in 2020 and caused disruption.

- Information-stealing Scams: These scams were designed by hackers to steal information from businesses and individuals. The websites used for this purpose looked real and seemed to provide legitimate information about COVID-19 but had malware embedded in reality. For example, a global map of COVID-19 cases was created with malware beneath it.
- Malware & Ransom ware Attacks: Hackers and cybercriminals exploited everyone's concern over the pandemic to introduce malware to the victim's computer and access confidential information in an attempt to extract monetary payment. For example, Hammersmith Medicines Research (HMR), a British research company, was attacked by the Maze ransom

ware Hacking group. As the company was gearing up for running COVID-19 vaccine trials, the ransom ware group released stolen medical records and asked for ransom which the company refused to pay.

- Vulnerabilities Around Work-from-home: With businesses running operations online, remote workers suffered from brutal cyber-attacks. The absence of security protections including firewalls and blacklisted IP addresses, home networks put remote employees at the risk of getting hacked and unknowingly provide the hackers with access to confidential files. For example, employees were provided with hacked conference passwords or links.
- Fake Products: Several websites were designed to sell fake products including coronavirus remedies, masks, and other protective gears without actually providing the user with any product.

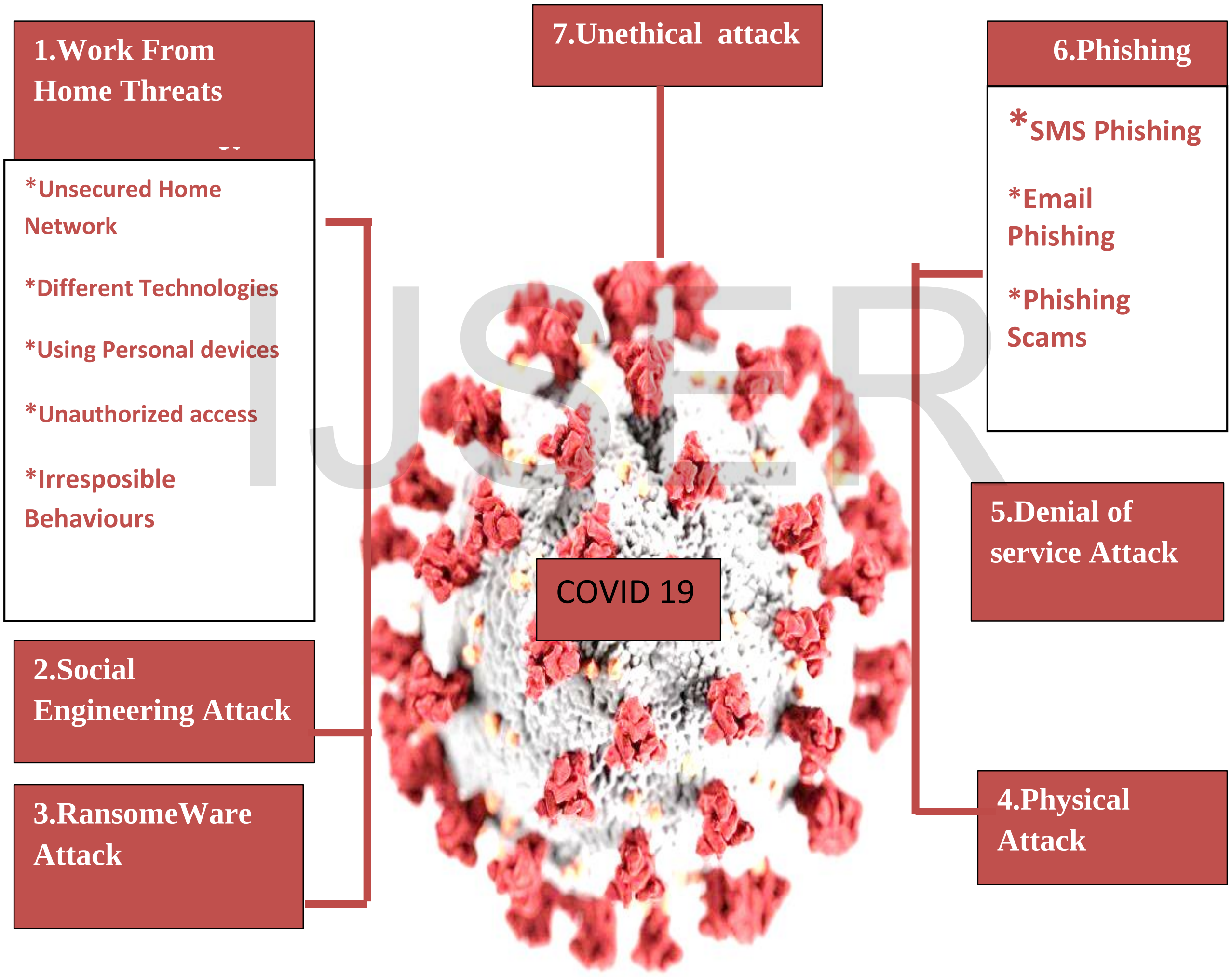

Fig 1 :COVID-19 malicious Cyber Attacks.

B.COVID-19 Malicious Cyber Attacks

1. Working from Home Malicious Cyber threats

The COVID-19 pandemic caused many citizens to work for the first time from home. Working from home has other cyber security threats, such as intentional cybercrime. When any personal computer or mobile phone is compromised, unauthorized access to the stored information can have a devastating effect on personal, emotional, financial, and working life

1.1.Unsecured Home Networks: As part of controlling of the coronavirus (COVID-19) spread, several organizations have encouraged or forced their staff to work from home. This presents new cyber security challenges that must be managed. During the pandemic, almost all employees are connected through their home network, which is not secure enough as their work network; therefore, they are exposed to risks**.**

1.2. Different Technologies: When working from home, different technologies may be available at home than those available at work. Several concerns must be considered, such as Poor Experience, Less Functionality and Productivity.

1.3. Personal Devices: When functioning from home, workers typically use their personal devices; likely, they feel softer mistreatment them. However, personal computers or laptops area unit terribly probably to exist.

1.4. Unauthorized Access: It is a very important downside that appened thanks to performing at home. The attackers still plan to access the system with none authorization.

1.5 Irresponsible Behaviors: The counseled securit ypolicy maywellbe desecrated once workers w orkfromhomeandfollow scatterbrained behavi ors like Untrusted Connections,unauthorized observance. Empl oyee Priorities.

2. Social Engineering Attack

The social inter fingering attack is another type of cyber security threat where malicious cyber actors use foundational social engineering techniques to enable a person to perform specific acts. Those actors leverage human characteristics such as interest and anxiety regarding the coronavirus pandemic to persuade possible victims. The uptick in socially engineered cyber-attacks is mainly targeted financial and personally identifiable information data.

3.Ransomware Attack

Ransom ware is a type of malicious money-extorting attack. In general, the malware operates by disabling the whole operating network or by encrypting a user's data, which allows the user to compensate for it. Attacks by ransom ware are primarily aimed at large organizations because they have a large volume and are ready to pay for them.

4. Physical Attacks

Several reports and news reached out to say that the commercial crime has been increased; these reports abstracted that in the following statement: "It seems like there are some folks out there looking to be opportunistic." They depend on the fact that people are already in panic mode and need assistance

5.Denial of Service (DoS) Attack

Denial-of-Service (DoS attack) is a computer attack in which the attacker attempts to momentarily or permanently make the services or Internet resources inaccessible to their intended users. Service denial is usually accomplished by flooding the target system or resource with superfluous requests for the intent of overloading and blocking the fulfillment of any or all valid requests .

6.Phishing Attacks

During COVID-19 time, the attackers send different emails or SMS messages with false claims such as having a "cure" or encouraging donation. Like other phishing schemes, these emails and SMS use real-world problems to try to manipulate people into clicking. The scam messages (or phishes) can be very difficult to detect and are intended to get people to react without thinking .Phishing attacks could be classified into three basic types: SMS phishing, email phishing, and phishing scams.

7.Unethical Attacks and Behaviors

Fear of the spread of the novel coronavirus and the severe losses it causes, whether in terms of human casualties or the economic crisis resulting from it and the accompanying extremely serious effects on the global economy, have led to a new “global information war” between countries in order to secure the necessary equipment to combat the deadly virus. Figure 21 shows the rate of the abused keywords related to COVID-19.

C.The case for increased cyber security

Due to increased network risks, the rise of remote work requires more attention to network **security.** For example, it is obvious from the fact that 47% of people fall for a phishing scam while working from home. Cyber attackers see the pandemic as an opportunity to strengthen their criminal activities by exploiting the vulnerability of employees who work from home and taking advantage of the high interest of people in news related to the coronavirus (such as malicious fake websites related to the coronavirus).

Due to the many opportunities that arose during the COVID-19 outbreak, most threats are increasing. One reason for the increase in 4,444 cyber-attacks may be because some small and medium-sized businesses adopted the "bring your own device" (BYOD) approach (as opposed to the "company owned company" (COPE) approach), which means that employees can use their personal devices (phones, tablets, or laptops) to access company information. Working from home does not guarantee the same level of network security as an office environment. When a personal computer or laptop is used to access company files and data (even with the security of an MDM solution), users are more vulnerable to cyber-attacks. For example, employees may simply not be able to run antivirus or antimalware scans on a regular basis. There are no complicated corporate prevention and detection measures in the home work environment. Additionally, home Wi-Fi networks are more vulnerable to attack.

Human error is another cause of concern. Before the pandemic, human error was the main cause of "network insecurity": employees contact the wrong people unknowingly or recklessly. However, in homework, the problem is even greater. When working from home, family members or social visitors may interrupt employees' work. These disturbances can make people more careless. IT systems must adapt to these changes in work practices and the increase in human error. This can be achieved in many ways, such as incorporating timeout information into key information systems, improving controls to apply the "four eyes principle", enforcing separation of duties (SOD) or automatic controls. After all, this is what "digital empathy" is all about.

D.A Far-More-Connected World

In just one month, the world has become more digital and fragile than ever before. In March, organizations that had been requiring employees to meet in the same location suddenly used the Internet to facilitate remote interactions between large groups of home offices. Internal employees of financial institutions have regulatory requirements to ensure that communications between each other and with customers are handled in a highly secure private infrastructure. Companies also rely on digital services to maintain their supply chains of essentials while minimizing social connections. officials rely on digital channels to assure and maintain order to the public. They are exchanging rapidly evolving rules, sharing important physical and mental health information, and flooding misinformation about rumors, fraud and false remedies. They are using these digital channels to urge employers to pay wages, while consumers must avoid accumulating food, medical supplies and personal protective equipment.

As Covid-19 proves the power of medical systems around the world, medical service providers are turning to chat portals, telephones, emails, and telemedicine for remote diagnosis and advice. Organizations are using digital infrastructure to procure vital protective equipment for health and sanitation workers and provide advice on how to provide services safely. Finally, digital channels provide entertainment for stressed families. They are motivating locked people to make the most of their time and provide tools to achieve this goal. They help support our future by allowing children to learn online while school is closed.

The increase in communications and the wholesale shift to online businesses have simultaneously increased the risk of cyber-attacks by an order of magnitude. They also introduced a variety of new risks. The perimeter security of the organization is at risk of being compromised. They need continuous monitoring and real-time risk analysis to detect violations of physical and digital entry points. Now, security and risk management leaders must protect their businesses on a large scale and quickly. They must ensure that their company's online services and digital platforms can withstand cyber-attacks. IT is also under tremendous pressure. In some companies, IT professionals must extend remote working capabilities to employees who have never worked from home in the past. In some cases, this includes your service partner. Many IT departments are implementing new collaboration software. Although this is essential for keeping employees (especially those in agile teams) synchronized, this type of software increases the risk of intruding sensitive data, which is now located in less secure remote workplaces. However, it is difficult for IT functions to refuse this. Business leaders, managers and their employees need access to internal applications and services to perform operations remotely. Since many companies have not previously provided these applications and data through the Internet or virtual private networks (VPNs), security leaders are reluctant to allow access without strict access mechanisms. Understandably, few organizations prepare their employees for large-scale remote work. They now realize that secure remote access capabilities and protected access to business systems have become major restrictions. Implementing corporate security policies and controls on remote workers is a difficult task. Most controls have limited scalability and require a lot of time to implement.

Cybercriminals are using the largest digital footprint and traffic to find loopholes or transfer funds. They launched Covid-19-themed attacks in the form of phishing emails with malicious attachments that initiate malware to damage the system or steal data and credentials. Attackers create temporary websites or hijack vulnerable persons to host malicious code. They draw people to these sites and then place malicious code on their digital devices. The fake website also uses e-mail links to solicit donations from daily wage workers. Some Covid-19 patient count status apps and links are loaded with identity theft viruses and malware. Remote work tools (such as video conferencing systems) have been hacked to find loopholes; Zoom's latest example is shocking.

E.A Robust Cyber security Response

In this new environment, cyber security professionals must actively respond to risks. For beginners, they need to quickly make the company's remote employees aware of the scam, and then train them so that they do not become victims. Online training or online learning platforms are very valuable here. But this is only the beginning. In addition, IT security professionals must pay attention to the mid-to-long term because they recognize that remote work has become the norm for many employees for a long time after the pandemic is over. An integral part of successful security work will be the implementation of effective and rapidly adopted technologies and solutions, such as those hosted in the cloud. Cloud-based security and platform services greatly reduce deployment time. They also enable companies to rapidly increase the breadth and depth of security protection based on current threats (so-called dynamic scalability). Cloud-based security also enables IT security professionals to manage all of this remotely. For example, cloud-based secure virtual desktop services enable IT professionals to remotely access employee systems, including files and networks. The cloud is also the key to a security system. Secure edge and cloud-based data leakage prevention and threat prevention controls can help protect the organization's critical assets. In addition, cloud-based hosted detection and response services can be extended to remote workplaces. In addition, companies that use secure remote access technology can provide remote employees with private access to business applications and systems (no VPN). Businesses can also use Privileged Access Management (PAM) services to allow special remote access to their IT and application administrators. Multi-factor authentication services, which include text-based and biometric methods, enable strict risk access based on internal applications that have been opened for remote access.

F A New Era for Cyber security

The changes we introduced will not only affect the IT department. If remote employees indicate that they are more effective at working from home, talent managers will need to review their policies to achieve better work-life balance. At the same time, people with key skills and remote working needs will need to quickly and effectively onboard. In addition, large companies will face new budget constraints. There will be new ways of using funds and investing in the right quotes. The company will allocate resources more strictly. is not only that, the company will have the opportunity to change the way of working. New work-from-home arrangements made during the lockdown period should be prioritized and shown to be good. Finally, as personnel, assets and facilities are restored, governments around the world will issue new policies and regulations based on their experience during the pandemic. As they adapt to the new post-crisis normal, organizations will also be forced to optimize costs and accelerate their digital transformation. Security leaders will need to use digital technology and transformed service models to do more with less to support these initiatives. The pandemic has ushered in a new era of network security. IT security professionals who improve the quality of games and protect company personnel, technology and data from new or increased risks brought by the most sophisticated cybercriminals will become key players in economic transformation.

G. Conclusion

Cyber security is on the agenda of most executive committee meetings, but given the growing threats during the pandemic, it may deserve more attention. In the second wave of coronavirus and the possible third wave of concerns, companies must actively respond to threats and plan methods to prevent successful cyber-attacks, rather than respond when they occur. However, although preventive measures are important, they also require cyber-attack detection, response, and recovery capabilities. The pandemic teaches us that being prepared is the key to successfully limiting the risks associated with cyber-attacks. The ability to respond quickly to unforeseen events helps reduce the impact of cyber-attacks. Companies that have benefited from secure remote work capabilities will be better able to respond to the continued increase in cyber threats. Companies caught off guard will have to quickly assess the risks of cyber threats they face and prioritize best practices to address cyber security vulnerabilities. When company data can be accessed from personal devices, cyber risks must also be assessed, and measures must be taken to limit exposure to cyber threats. The reality is that companies must change their views from "if" to "when" and recognize that the consequences of data privacy leaks or ransom ware may cause economic losses. It should also be remembered that economic gains are not the only cause of cyber-attacks. "Hacker activism" and its goal of damaging business reputation is an additional threat. There are many ways to reduce the possibility and impact of cyber-attacks, but they require targeted actions and plans. Companies must make their remote work practices resistant to cyber-attacks and improve the development and implementation of security measures

References

1.Rabie A. Ramadan,2021" Cybersecurity and Countermeasures at the Time of Pandemic"2021

https://www.hindawi.com/journals/jat/2021/6627264/

2.P. Roberts, "More scam artists go phishing,"2004,

https://www.pcworld.com/article/116330/article.html.

3.Daniel Lohrmann, Dan Lohrmann "2020: The Year the COVID-19 Crisis Brought a Cyber Pandemic"https://www.govtech.com/blogs/lohrmann-on-cybersecurity/2020-the-year-the-covid-19-crisis-brought-a-cyber-pandemic.html

4.https://www.securityroundtable.org/managing-cybersecurity-in-a-time-of-pandemic/

5.https://www2.deloitte.com/ch/en/pages/risk/articles/impact-covid-cybersecurity.html

6.S. Shira and J. Jennifer, "Cyber-attack hits U.S. Health Agency amid COVID-19 outbreak," 2020, https://www.bloomberg.com/news/articles/2020-03-16/u-s-health-agency-suffers-cyber-attack-during-covid-19-response.

7. C. Cimpanu, "Czech hospital hit by cyberattack while in the midst of a COVID-19 outbreak," 2020, https://www.zdnet.com/article/czech-hospital-hit-by-cyber-attack-while-in-the-midst-of-a-covid-19-outbreak/.

8. https://www.cfr.org/blog/2020-review-covid-19-pandemic-and-cyberspace