COVID 19 PANDEMIC: IMPACT ON BUSINESS AND CYBER SECURITY CHALLENGES

[1.]Dr. Archana Sharma , [2.] Purnima Gupta
[1.]Associate Professor, [2.] Assistant Professor,
[1]. IT Department, [2.] IT Department,
[1.] IMS Noida ,Noida, India [2].IMS Noida, Noida, India.

Abstract: The COVID-19 outbreak is a massive compassionate emergency that has also rigorously affected the worldwide economy. The rapid and unpredictably broad distraction to businesses around the world has left companies struggling to sustain security and business stability. As businesses/organizations have shifted to remote functioning to safeguard their employees while continuing to serve their customers. Companies have moved the majority of their actions to the digital world which leads to the high risk of cyber attacks. There are few challenges that how to secure this remote working practices while ensuring essential business functions are operating without any disruption and further how to keep the organization protected from attackers by taking the advantage of the uncertainty of the situation. The research explores the current trends of cyber security threats during the pandemic and further highlights the impact of COVID -19 on global business environment and the various types of cyber security challenges have to face by business leaders and the individuals with the preventions may be taken organizations to protect the business from the security breaches.

Index Terms: **Phishing Attack, ransomware, maze, corona virus, emotet, trickbot, EDR.**

I. INTRODUCTION

Pandemic which has been really considered as a worldwide cyber pandemic initiated 20 years ago. Till date, cyber crimes have expended exponentially and multiplied to every place of across the globe. A person's data is expected to be infected online by physical existence in either any area like Southeast Asia, eastern Europe or Africa. This global cyber epidemic has been accelerated speedily by states. Over the past 20 years, cyber capabilities have frightening new mechanism of national power. The COVID-19 pandemic has altered the way business is done around the world. With mostly remote personnel operating on unsecured networks at home, business security players are struggling to control of speedily growing attack areas. Cybercriminals along with the state-sponsored highly developed threat groups take advantage of the COVID-19 pandemic for attacking the networks across the world to get the benefit of monetary and the intentional gain. Between January and March 2020, corona virus-themed phishing allure, various malware contamination, network infringement, rip-off, and disinformation battles have become uncontrolled across the clear, profound, and murky web. This research to explore the most prevalent COVID-19 cyber threats: phishing websites and emails, fake corona virus mobile apps, malware, ransomware, fraud, and disinformation. It also addresses the criminal and state-sponsored threat actors behind these campaigns, the most common types of targets, and network indicators of compromise.

The FBI look forward to cyber player with the excessive use of virtual environments by various government sectors, the private organizations and individuals due to the impact of COVID-19 pandemic[1]. As Computer systems, Smart phones and virtual environments endow with necessary communication services for remote work and education, in addition to carry out normal business. Cyber players take advantage of vulnerabilities in these functional systems for unauthorized access and lift the sensitive or confidential information, target the individuals involved in passing data over network and financial transactions performed by industries. A threat of troublesome and destructive attacks have been targeted to organizations across industries and geographies by various targeted ransomware incidents.

Initiation with simple phishing attacks and hand sanitizer scams now several predictable threat player have become more active in COVID 19. APT36, FIN7, the Maze ransomware group, and several other country state players are now at the back attacks related to the coronavirus pandemic. As sophisticated threat players enter this loop, both the volume and sophistication of the cyber attacks will probable increase in future.
The research suggests the following steps for resistance against these threats:

- Update the present threat countryside risk measurement based on new budding threats to remote workforce.
- Intimately supervise collaboration and remote working platform.
- Stringently enforce the use of VPNs, security measures like encryption and endpoint security also.
- Impose strong password policy and two factor authentication.
- Educate the employees and individuals on the new cyber threat landscape.

II. SECURING THE NEW REALITY IN COVID 19

There is a transformation in work of individuals due to COVID and enforced the way organization working culture, the completion of projects which might have been of about a year duration now have been motivated to finish within weeks. Practicality has been considered as a rule, with the acceptance of this reality , business organizations have taken the various cyber security risks also which might never have established in other situations. Structured cyber crime clusters have shown themselves merciless and industrial in taking advantage of fear, uncertainty and uncertainty over COVID-19 —deliberately phishing and attack communications to build out COVID-19 forged websites and evade. States themselves have personalized their own cyber surveillance strategies.

The impact of COVID-19 on the universal cyber security marketplace is expected to raise from USD 183.2 billion in 2019 to USD 230.0 billion by 2021, at a Compound Annual Growth Rate (CAGR) of 12.0% during the estimated time. The marketplace expansion can be accredited to upward focus on securing remote communications or infrastructure and IP of organizations due to work from home and various remote service activities and schedules. For all businesses, the key focal point should be on cyber security instead of just as a sustain function to drive the marketplace with a higher holder share for cyber security guidelines and infrastructure.

2.1 Different types of Cyber Attacks Active in Pandemic COVID 19

Cyber security is really becoming a apprehension for organisations that how to sustain the security of data and adopt the new working culture in this changed world after observing the rage of Corona pandemic. This amplified remote working cultures has now made business enterprises with higher vulnerability for Cyber threats and attacks. Thus to overcome with this situation, IT professionals of all kind of enterprises and start-ups are now drawing some additional cyber security policies for the to improvement of their IT infrastructure.

2.1.1 Phishing Attacks

Most of the companies and organizations of private sectors practicing this change in their working culture lately just because of COVID-19 pandemic. Remote activities like tele working are increased .It is mainly reliant on E-mail for message communication, which leads to email fraudulence activities [3].

Cyber criminals are captivating benefit of the COVID pandemic by spreading the awareness of the Corona as subject to dodge users into enlightening their personal details or clicking on malevolent attachment or links, unintentionally downloading malware to their systems[4]. These security breaches may even pretend to be with any public or private sectors, health ministries, or any reliable sources or figures in any country. Such emails seems to be authentic including logos or brand name of the particular organisations. According to Barracuda Networks , a foremost provider of cloud-enabled security and data protection solutions report[5], the diversified phishing movement are taking benefit of the susceptible centre of attention on COVID-19 to share out malware, whip credentials, and cheat users out of money.

The general phishing strategies have been observed for such cyber attacks. Moreover a large number of movements are using the corona virus to attract and use a trick for unfocused users to take the benefit of the fear and uncertainty of their projected victims. During March 1 to March 23, the research detected 467,825 email and phishing cases, out of them 9,116 were associated with to COVID pandemic [6]. The figure 1 shows the analysis of emails sent during Jan. 2020 to May 2020 related with the COVID-19 threats.

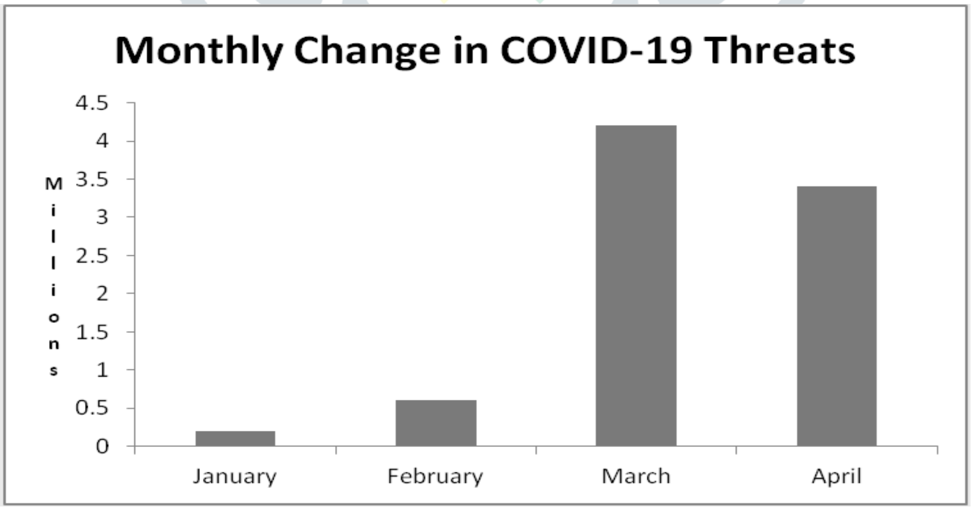

Figure 1: Analysis of 1 billion emails sent between 1 Jan., 2020 – 1 May, 2020

"All COVID emails does not include emails referencing Coronavirus/COVID-19 in the email body but not in subject area"

While analyzing the threats, it has been observed that malicious groups generally trust on masquerade tricks like "official" communication through HR representative or executive or create the URLs like WHO, CDC etc. looking for the credentials or confidential information or financial details. Most of the time COVID -19 have been used by cyber criminals to build ransomware and threat of phishing.

2.1.2 Malicious domains

For malicious activities over internet related with COVID-19, cyber criminals registered various domains containing the terms like corona-virus, coronavirus, covid-19 and covid19.Although, there may some legitimate websites also. For masquerade and spam drives, cyber criminals create thousand numbers of new websites regularly. By taking the benefit of worldwide communication on COVID pandemic, cyber criminals embed the Malware, Trojan and Spyware in interactive corona websites and maps of corona virus.

2.1.2.1 Remcos RAT Malware

An executable file "CoronaVirusSafetyMeasures_pdf[.]exe."[7] is dropped as unidentified contamination vector to spread the Remcos RAT malware. It persist during the start up key to permit the malware to restart and installs a Remote Access Trojan as the victim start the system again and malware logs the individual's keystrokes and command IP. Due to COVID -19 spam cases have been increased in large number and threaten with COVID -19 in failing to pay a ransom amount. The demand of ransom in bitcoin as $500 or threat of corona virus in next 72 hours and the emails come into sight to be sent from the victim's legitimate account. In most of the cases the IP addresses are of East Asia[7]. Seqrite, a cyber expert on May 18 reported that to target the specific Co-operative banks in India, a unknown corona virus based emails were claimed to be from Reserve Bank of India.

2.1.2.2 Lokibot

To lift the data and email credentials like user id and passwords to FTP server and crypto coin wallets, a another kind of malware Lokibot has been activated and distributed in unlike corona pandemic related phishing movements.

The FortiGuard Labs of Fortinet, a security firm released a report and revealed that the spear-phishing movement is spreading the Lokibot , a email credential stealer by taking the benefit of fear of COVID -19[8]. Spear phishing emails are generated in English with abundant grammar and lots of spelling mistakes. The report further highlights that once the attachment file is opened and decompressed , a another file with the name"DOC.pdf.exe" displayed and if it opened, this file projects the Lokibot within the infected system.

2.1.2.3 Trickbot

Trickbot initially treated as a Trajan for banking, but now it has been re-treated as one of the advanced and proficient form of malware spreading around the world. Since the starting of the year 2020, the check points at various location has found at most, 4000 COVID-19 associated registered domains globally whereas 13% of them were initiated as malicious and 5% in addition to found suspicious and investigated[9]. It has been observed that Covid –connected domains malicious rate is increasing speedily

2.1.2.4 Emotet

Emotet permits cyber attacker to steal confidential details or money of victim's computer system or mobile device as infected by it. In this pandemic situation, Emotet spreading the cyber scams as it is self propagating malware and being used as dropper to dispense ransomware and other malware which will take the hold of the targeted system for stealing the confidential information, execute the crypto jacking fiddle or may catch it for ransom[10].

As a Trojan, Emotet is initially spread through malspam mails which may enter to the victim's system through various ways. It may be malicious link, malevolent script, document file with macro. Emotet infected emails may associate similar branding design seems to be the legitimate mail. It may also persuade the end users to click the infected files with the use of attractive language like Payment Details, Invoice Details etc[11]. Emotet is very difficult to identify as it applies indescribable techniques to evade detection, as dynamic link libraries. The one of the case of phishing movement was to target the Healthcare on 22 April, 2020 Emotet Botnet which shows the Signs of Life & COVID-19. It has been concluded by DHS that this Emotet malware is one in the majority of destructive and costly malware which spreading the infection in all types of organization as public or private, government, individual and costing very high to clean up as $1 million per confrontation[12].

2.1.2.5 Formbook

Formbook malware with the data stealing capability from the web browsers and number of other applications also. In a research of malicious attacks of COVID –related campaigns, both Trickbot and Formbook attacks have been seen in a large number, specially in May, 2020[11]. An email movement pretending to be the information about the corona virus latest updates from WHO(World Health Organiation) is spreading a malware downloader to install the Formbook Trojan to steal the information. This email also contains a attachment as ZIP file with a statement from "World Health Organization" and the ZIP file contains the "MY-HEALTH.PDF" which was attaché for the phishing purpose only. Although it will pretend to user about the latest update about the corona virus statewise. The formbook malware as downloaded to the system put efforts to steal the contents of log, Windows clipboard, keystrokes and web browsing data.

2.1.2.6 Ransomware

Another type of malware, ransomware usually encrypts the data and blocks the accessing of computer system and demand the payment to pay to the attacker with deadline sometimes. In case of no payment in time, the data may be lost forever. Different kind of organizations, consumers, hospitals, public institutions, medical centres and industries are being under attack by ransomware. Due to health disaster they are not in position to locked out their computers ensures the cybercriminals that victims are interested to pay the amount demanded. Sophos, a security firm revealed the analysis on ransomware attacks in May, 2020 including the 5000 IT managers accorss the globe. It was observed that more than 50 percents of the surveyed organizations were attacked by ransomware[12]. In U.S, the estimated ransomware cost of year 20202 could be approx $1.4billion. This number could be increased by adding the cost of downtime and revival by $9 billion in 2020. Approx. $111000 was the average amount of ransomware attack on enterprises in Q1 of year 2020 and $40,000 was average ransom imbursement[13].

2.1.2.7 Maze Ransomware

The Maze ransomware generally hits the organizations and companies by infecting the corporate network and computers with windows os. It encrypts the data and block to unable the accessing by end user for ransom demand. As the COVID-19 is being speed up across the world , the maze ransomware attacks has also increased in various IT companies like Cognizant, Conduent etc. The foremost feature of this malware is that malware creator threaten to the victims for ransom payment otherwise the information would be released over open network. Initially some cyber criminals had promised to not consider the medical services during this pandemic, but few didn't agreed for it . Maze attacked the US Law companies, German administration, HMR company. HMR company carry out the clinical test and prepare the vaccines for corona virus. On 14th March, 2020 , this company was attacked for 2,300 patient medical records and on 21st March, 2020, employees details were leaked.[14].

2.1.2.8 NetWalker Ransomware

Mailto malicious software (Net Walker Ransomware) was revealed by GrujaRS and restructured version of Kokoklock malware. The main feature of mailto malware is to encrypt the files and reproduce them by renaming them to make unusable for victim with the creator's mail address and victim's distinctive ID as extension[15]. The Netwalker group are not hesitating to exploit the COVID -19 outbreak by infecting the computers of the individuals and entities who are involved in health organizations or health service industry. The disillusioned emails sent by this malicious group masquerade themselves to represent associated with corona virus disaster but as the recipient click on the attachment file of Excel or Word file, their systems get infected.

With the subject corona virus, phishing mails were sent with the malevolent attachment with the name "CORONAVIRUS_COVID-19.vbs" which contained the embedded NetWalker malware execulable file in starting of March, 2020 to various organizations[16]

2.1.2.9 Extortion and Fear Tactics Through Ransomware

The conventional cyber-criminal groups are still sustained with the art of theft of credit cards and individual information for a simpler approach called cyber extortion. Under this, Victim's money is demanded instead of stealing it. Cyber extortion persist to put on grip just owing to millions of dollar criminal business. Regardless of law enforcement of governments and healthcare industries, could not run away of its conduit[17]. The cyber attackers are taking benefit of people's fright just about the COVID-19 for ransom money.

2.1.3 Palo Alto Networks Tracks Cloud Threat Landscape

The researchers have found 1.2 million domain names registered with the keyword associated with the name COVID-19 of Palo Alto Network of Unit 42 during 9th March to 26th April, 2020. It was found that approx 86,600 of the briefed domains are malicious. The highest figure of malicious domain in United States (29,007) with the trail of Italy i.e 2,877, Germany -2,564, Russia as 2,456[18].

End point security and unremitting threat scrutinize products are being sold by security retailers as well as PaloAlto Networks to prevent employees automatically as they visit such type of malicious domains. In addition to these security instruments, it has been observed that employee education regarding cloud based threatening also required as unknown file click could be a malicious movement[19]

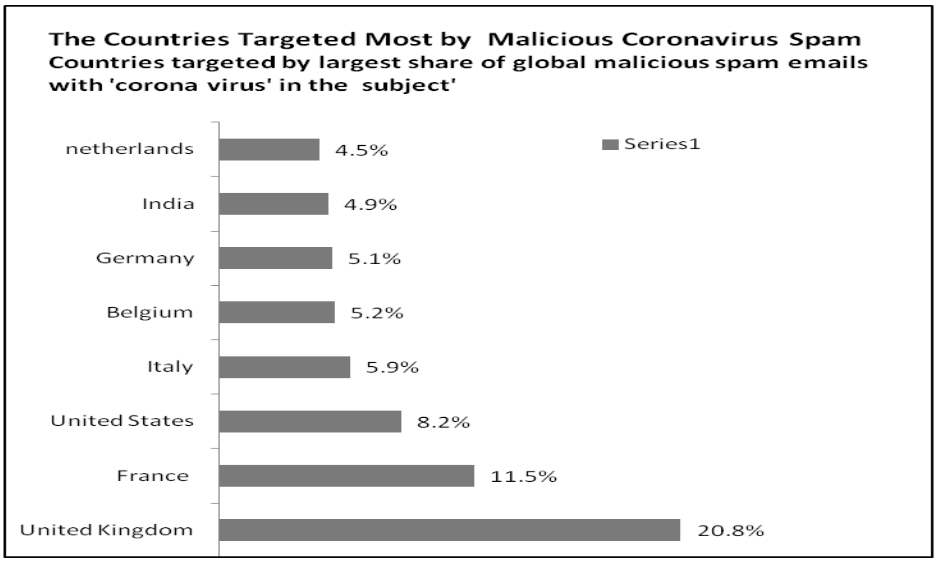

Figure 2: Malicious Coronavirus Spam (January 1 to March 27, 2020, Source Trend Micro)

III. CYBER SECURITY THREATS TO INDIVIDUAL AND BUSINESS ORGANIZATION

Unfortunately fraudsters have a tendency to wish on unpredicted challenges or events. Due to disruption of normality they look for an opportunity which may exploited. Fraudulent activities have significantly increased due COVID-19 pandemic. For most of the people life have become very tedious and unusual and more at risk while work from home, financial crisis, future prospects etc. Retailers and other businesses are also facing significant uncertainties over cash transactions and revenues, international trades.

3.1 Individual and Private Banking Customers

The private and individual banking customers are natural aim for cyber criminals. It has been observed that the 'phishing' cases associated with COVID-19 increased, the emails seems to be from bank for financial help available due to pandemic, but unfortunately these mails may contain suspected malware that are downloaded onto the customer's computer once clicked the link. Call centres frauds are also increased. Proactive actions of bank are making the customer aware about the security of the system and guiding them about the phishing attacks.

3.2 Challenges of employee remote connection

However, Banks are not only concerned and strive hard for customers to protect from cyber criminals, the risk has increased for staff also. It may be just because of unintentional consequences of bulk movement of employees to work from home that cyber criminals have become more active and phishing mails and scams have been increased. At the same duration most of the working family members share the same network while doing their official work and download the contents with click invites the malware at their system and could take entry in the firm also if the end point security is proper. The eavesdropping or take control of the conversation in case of video conferencing also has been increased in this pandemic time.

3.3 Trader surveillance intermittent

Trading is the another area where surveillance is required and monitoring as well as recording of also required as per the regulatory guidelines. The other area of surveillance is Trade. According to the regulatory rules, the recording and monitoring of traders call are essential. Unfortunately, now Tader's calls are unrecorded due work from home and pandemic situtuation.

The impact of Corona virus on Trade in India have estimated approx 348 million dollars, according to United Nations report, in addition to it the country has been counted among major 15 financial market which have affected due to china's manufacturing process slowdown as disorder of china international trade[20].

3.4 Healthcare Sector Challenges

In COVID-19 pandemic situation, as all hospitals, health care workers, doctors and staff looking after the patients while in other side of the world, the cyber criminals are looking for the exploitation of this pandemic outbreak[21]. The healthcare segment have been facing the new challenges in COVID-19 pandemic due to strong data integration and IT infrastructure. Although it is positive but invites the network vulnerable to various types cyber attacks like, ransomeware, email phishing, network data breaches due IT as a backbone of healthcare sector now a days. The major target areas are Laboratory management system, Hospital record system, Individual health record, radiology information system and email servers. The cyber criminals also focus on endpoint devices which involves the patient monitoring kit that are generally connected to the internet.

3.5 Manufacturing Industry Challenges

Supply chain security has major issue of cyber threats globally in COVID-19 outbreak. The supply chain integral process mainly dependent on data process by suppliers or services provided them. Due to corona virus and related global lockdown, the drastic risk of short and long term have been causing in companies supply chain process. The cyber security risk have been increased at present due to organizations trust on most of the suppliers with confidential and sensitive data[22].

The research highlights the other key aspects to be focused by suppliers that :

Multi factor authentication has not been enforced while remote access of services, No formal agreements have been put by some of suppliers to restrict the third-party deployment of data, No data security training is being provided to the some supplier's employees, lack of penetration tests of IT infrastructure which are directly connected with public.

IV. CYBER SECURITY BREACHES PREVENTION TECHNIQUES FOR BUSINESS ORGANIZATIONS

To prevent the business organizations from cyber security breaches, Endpoint security is must as a solution which includes the Endpoint Protection along with Endpoint Detection as well as Response solution. These two solutions together secure the remote devices employed in organizations and endpoints from various malwares, Trojans as well as other unknown advanced threats. Endpoint Detection as well as Response solutions allow unremitting detection and quick response in case of any unknown cyber security threats and monitoring of cyber security.

In case of major workforce of organization working remotely, there is a need to focus of data privacy and cyber security mainly on the below mentioned four areas which are generally to vulnerable to a breach are This may support to ease the breach happening in reality and restrict any possible liability.

There are four major areas has been highlighted to remain the business secure from cyber criminals and data violation during the noisy time.

4.1 Email Security

It is very much essential to know for all individuals about the email security. Most of the attacks are happened through email only in this COVID-19 pandemic. The person should avoid to open the suspicious or unknown emails, downloading the unexpected attachments. Verification of suspicious attachments or links is required before open it through any other mode of communication like text message. Never provide the personal details to unknown suspicious resource like birthdate, password or social security number. Be aware with emails of poor grammar or poor design as it can be a phishing attack.

4.2 Password Protection and Multi-Factor Authentication

Always strong password should be set on all employee's and individual's account. All individuals should avoid password which may be easily identified like birtdate, pet name, spouse name etc. Such password are attempt of Brut Force attack.

4.3 Web Safety

As the research highlighted, in this COVID-19 pandemic massive invasion of bogus websites, whose developers are looking for the opportunities by taking the benefit of fear in nearby of coronavirus. Always ensure that any site looking for require the account personal details like username and password. In case of financial transaction, a valid encrypted digital certificate is associated to ensure the data security. Secure websites always begin with "https". Remote workforce should avoid the public systems and Wi-Fi connectivity for accessing the confidential information. Always sign out all accounts and shut down the device either computer or mobile device when it is not functional.

4.5 Device Maintenance

As various cyber criminal groups are active during COVID-19 outbreak, thus there is a need to keep all resources like hardware, software etc updated with latest versions. All Employees should take the regular backups with multiple copies of all important and critical data and keep safe away from the network from the ransomware attack or unknown malware attacks. Such kind of prevention will allow to maintain the data protected from malware attacks. There must be cyber insurance policy of the organization.

4.5.1 Identify supply chain risk

A supply chain build up with various activities in manufacturing process which includes the transformation of usual resources, material in raw form and components finally into a complete or finished good that is to be transport to the customer. Thus in this CONID-19 situation, Business need to identify the loose end points while workforce working remotely. When any link within supply chain process fails, the entire business process disrupted. The post effects of it may be in inflation of costs, reduced revenues, reduce customer assurance, market share down.

V. RESHAPING THE BUSINESS MODEL AS CYBER SECURITY SOLUTION

As the demand of the current scenario during COVID -19 outbreak to reshape the functionality of the organizations in an innovative way with the mixture of work from home and office of the employees. To communicate and access data remotely over email, strong network connectivity is required. Additional dynamic authentication need to added as cyber security solution. The additional Cloud security alternatives is essential. Few organizations under COVID -19 cyber attacks now come up to re-examine the detection of cyber security infringe and scam control algorithms, modernize the IT infrastructure for the revised hybrid functional models.

There are some learning around flexibility from COVID-19. The current situation of corna virus enforced the organizations to reshape their business models todeal with hybrid functionality of workforce, maintenance of customer demand and fulfilment at supplier end. Companies have been forced to create and mange crisis management alternatives and handle it with pace. All individuals should learn these matter to face all kind of situations.

CONCLUSION

The protection of business as well as individual counter to cybercrime in the situation of COVID 19 and economy will be a top-down practice in this situation where the government leading role is required. Earlier, the Cyber threat was considered as the state tools and has vision cybercrime just for threat in case of only its engagement in espionage. Complicated security breach that wring individual person and different service providers like public or private has diminished between the gash in law enforcement retorts. This unresponsiveness is not conscionable more due to the exponential growth of ransomware with the support of cyber hackers to attack the various healthcare systems at the critical time of Corona outbreak. This research focused on cyber security challenges during the COVID -19 pandemic situation and various types malware and ransomware active to threat the business organizations and individual for their confidential information spread over internet. There is a need to measure the incidents and responses in addition to anticipatory measures. As the research highlighted the few measures may be considered by business, various industries, trade, banks and other private sectors and individuals as number of remote workers have increased due to corona pandemic and reform the business model as the safety measure.

REFERENCES

[1] www.fbi.gov/contact-us/field
[2] Covid-19 Impact on Cyber Security Market _ Coronavirus Outbreak & Cyber Security Industry _ MarketsandMarkets.html
[3] Covid-19 ignites a firestorm of cyber attacks
[4] https://www.interpol.int/en/Crimes/Cybercrime/COVID-19-cyberthreats
[5] https://ciso.economictimes.indiatimes.com/news/covid-19-related-phishing-attacks-up-by-667-report/74839322
[6] https://www.interpol.int/en/Crimes/Cybercrime/COVID-19-cyberthreats
[7]https://enterprisetalk.com/coronavirus-crisis/ibm-x-force-study-coronavirus-themed-spam-records-14000-spike/
[8] https://www.bankinfosecurity.com/spear-phishing-campaign-uses-covid-19-to-spread-lokibot-a-14058
[9]https://www.zdnet.com/article/trickbot-malware-is-using-these-unique-macro-laced-document-attachments-with-a-coronavirus-theme/
[10]https://www.livemint.com/technology/tech-news/phishing-scams-on-the-rise-amid-panic-over-covid-19-11583424287780.html
[11] https://www.malwarebytes.com/emotet/
[12]https://www.willistowerswatson.com/en-IN/Insights/2020/04/keeping-vigilant-against-increasing-cyber-risk-during-Covid-19-crisis
[13] https://securityboulevard.com/2020/05/covid-19-uncertainties-fuel-ransomware-attacks-and-phishing-schemes/
[14] https://www.bleepingcomputer.com/news/security/maze-ransomware-demands-6-million-ransom-from-southwire/
[15]https://www.incibe-cert.es/en/blog/netwalker-ransomware-analysis-and-preventative-measures
[16]https://www.tripwire.com/state-of-security/featured/netwalker-ransomware-what-need-know/
[17] https://www.cisecurity.org/blog/cyber-extortion-an-industry-hot-topic/
[18] https://unit42.paloaltonetworks.com/covid-19-cloud-threat-landscape/
[19]https://www.sdxcentral.com/articles/news/mcafee-crowdstrike-palo-alto-networks-track-evolving-covid-19-cyberattacks/2020/05/
[20] https://economictimes.indiatimes.com/news/economy/foreign-trade/trade-impact-of-coronavirus-epidemic-for-india-estimated-at-348-million-dollars-un-report/articleshow/74487020.cms?from=mdr
[21] https://www.aha.org/news/blog/2020-03-19-four-ways-mitigate-covid-19-cyber-risks
[22] https://www.cpomagazine.com/cyber-security/supply-chain-security-on-thin-ice-in-the-age-of-covid-19/