Economic Impacts of Post Pandemic Cyber Crimes – A Global Overview

[*]**Anirudh Bharadwaj M,**

Abstract

Cybercrimes have become as common as petty crimes and at every level we can face situations that make us vulnerable to cybercrimes through links, text messages on phones, scam phone calls etc. that demand to sensitive information and misuse them. The 2019-2021 Corona Virus (SARS-CoV-2) Pandemic has shown a drastic increase in cybercrimes. As use of technology, remote access work and communication rise, increase in digital process increase, it has also made people vulnerable to many different types of cyber-attacks such as phishing, malwares and social engineering. It has also resulted in commercial theft of intellectual property. This paper tries to throw light on economic loses that have occurred due to cybercrimes.

Keywords: Cyber Crimes, Corona Virus, Cyber Attacks, Phishing.

Introduction

The world witnesses the COVID 19 pandemic in the year 2019 caused by the Severe Acute Respiratory Syndrome Coronavirus 2 (SARS-CoV- 2). The first case was discovered in Wuhan, the capita of Hubei Province in the People's Republic of China. This virus resulted in the deaths of nearly 2.47 million deaths as of February 2021. It affected more than 110 Million people in less than a year. The world health organisation in the month of February 2020 called it a global pandemic and advised the countries to restrict mobility and avoid physical contact. Lockdowns were implemented across many countries of the world as a restrictive measure and face masks were made mandatory for any form of mobility in the public. The world health organisation also laid safety measures regarding physical contact and rules of sanitization and oral hygiene. It was very challenging for countries to transform the style of operations in each and every aspect of daily lives.

Trade, Commerce and Businesses were severely affected during the pandemic as there was difficulty in transport and mobility. According to the International Monetary fund, the world nearly lost 28 Trillion US dollars during this Pandemic.[1] The world had to strategize trade, commerce and business in order to cater the needs of the people. During this time, the internet came out as one of the most powerful tool as this enabled businesses and commerce to take place online which minimised the contact between people and reduced mobility. This study tries to analyse how the increased trade, commerce and businesses that took place online created vulnerability, increased risks of cybercrimes and attacks and the study tries to provide an overview of how the world tried to tackle the challenges in most prominent regions. This study tries to throw light on how the risks of cybercrimes created loss in business around the world. Also, see how nations are adapting to the new environment post pandemic where the risk of cyber security is high and tackle this challenge through legal and legislative measures.

This study considers major regions of the world that are most affected by cybercrimes Asia, North America, Europe and Africa. These continents are severely affected as they have recurred at many regular intervals. This recurrence is popularly known as 'waves'. Europe in the year 2020 saw its second wave, Sue to the density of population, India and USA saw a long rising slope before the corona virus vaccine was introduced. As of February 2021, nearly 28.3 million people have been affected with more than 500,000 deaths. The number of cases peaked on 8th January 2021. On the same day, nearly 300,000 cases were added and slowly, it has gradually decreased to nearly 70,000 cases per day. In India, nearly 11 Million people

[*] **M.A, Charles University, Prague, Czech Republic.**

[1] Initial Output Losses from the Covid-19 Pandemic: Robust Determinants. (2021). Retrieved 4 March 2021, from https://www.imf.org/en/Publications/WP/Issues/2021/01/29/Initial-Output-Losses-from-the-Covid-19-Pandemic-Robust-Determinants-50025.

have been affected. Around 150,000 people have been killed from the virus. The corona virus cases peaked on the 17th of September and it added nearly 98,000 cases and it started reducing after. As of February 2021, India is seeing a weekly average of 13,000 cases per day according to the Corona Virus Indicator.

Cybercrime and crisis situations

Cyber Crime by nature uses computer and a network. It uses the network as a tool to use to breach information of another person, organisation or a state. Numerous types of cybercrimes have taken place from the time computers have been taking place since the invention of networks. It is generally used to breach confidential information associated with an organisation or an individual. Some of the common methods of cybercrimes include Phishing, Social Engineering, Remote Access Trojan and Ransom ware. These days some of the most common attacks also include Cyber extortion, Identity theft and Software Piracy. These attacks have been increasingly common during different crisis situations where people have witnessed losses of millions of dollars, loss of personal information, theft of intellectual property such as software, e-books, audio visual content such as films, documentaries and academic materials such as research papers. These are some of the common methods of cybercrimes. There are legislative measures taken in different countries which penalises the people who indulge in cybercrimes. This paper tries to study different types of cybercrimes that occurred in 4 major continents of the world.

Phishing attacks: Phishing is a type of cyber-attack where a person or a group of people disguise as trustworthy people to steal sensitive details (Ramzan, Zulfikar 2010)[2] The Phishing attacks are used to steal important financial information of people by sending them fraudulent emails, links or messages by which the receiver usually gives out sensitive information such as password, bank account details, card details and other such personal information. According to Cision, A news distributing agency in USA, they found out that nearly 1 in 4 Americans received a phishing email during the pandemic. This was due to increase in the activity online such as shopping and working. It was also reported that more than 20% of the USA’s companies increased training programs to be aware of cyber security.[3] According to security experts at Kaspersky, Nearly 2 million phishing attacks were recorded in Africa in countries like Nigeria, Kenya, Egypt and South Africa, The reason was also because that pandemic raised the risk of phishing attacks in Africa as the attackers used it as an excuse to attack people.

Social Engineering: Social engineering is the method by which a person is forced to perform certain actions by manipulating their behaviour. It may be through asking them some sensitive information regarding security questions on the internet, sending them fraudulent phishing emails by promising some kind of support in online services such as banking, computer service. The most common form of this social engineering is by using the password altering options, to reset the password, somehow manipulating people to give out the security questions and getting into the account of the people and getting into their social media or financial accounts. According to Venkatesha, S., Reddy, K.R. & Chandavarkar, B.R, there has been incremental messages during pandemic that aimed to steal sensitive information of people by sending them emails asking for sensitive information. They talk about the measures taken by the government of USA and their notification that was sent to people regarding various malicious emails pretending to be doctors, hospitals and other organisations pretending to be active helpers in pandemic situations. [4] The united states government officials warned the people not respond to mails that pretend to be an authority claiming to help during the pandemic, forcing them to respond to them in limited amount of time, messages that are spreading panic mails or mails that provide false hope to people and those mails that indicated some kind of scarcity

[2] Ramzan, Zulfikar (2010), "Phishing attacks and countermeasures", In Stamp, Mark; Stavroulakis, Peter (eds.), *Handbook of Information and Communication Security*, Springer. ISBN 978-3-642-04117-4.

[3] Corporation, O. (2021), Phishing in a Pandemic: 1 in 4 Americans Received a COVID-19 Related Phishing Email. Retrieved 28 February 2021, from https://www.prnewswire.com/news-releases/phishing-in-a-pandemic-1-in-4-americans-received-a-covid-19-related-phishing-email-301134037.html

[4] Venkatesha, S., Reddy, K.R. & Chandavarkar, B.R. Social Engineering Attacks During the COVID-19 Pandemic. *SN COMPUT. SCI.* **2,** 78 (2021). https://doi.org/10.1007/s42979-020-00443-1

such as tickets or cure for medical conditions.[5] Kaspersky documented an increase of people involving in social engineering and phishing attacks keeping the pandemic as a reason to provide services. They also warned the people to secure their information so that they are not misleading to giving criminals with sensitive information.

Software Piracy and Other Intellectual Property Piracy: Software piracy is a method by which people duplicate the licenced software, new books, textbooks, research papers, films, documentaries and other content and release it unofficially into different public domains in the forms of links, downloadable items on torrent websites and other unofficial sources of the internet. This causes huge financial losses to the creators of this intellectual property. If people get easy access to such intellectual property such as books, research papers and textbooks, the students and other academicians will download it unofficially, which will result in the loss of income to the publisher. Piracy and duplication of films and documentaries are not new to the world as websites such as Torrents, The Pirate bay and Mu Torrents have been one of the most popular sources to download films, software and intellectual property such as books. The Pirate Bay website also had been charged with piracy charges and the European Court of Justice ruled that it is creating infringement of copyright and crating loss to creators of these intellectual property rights. [6] According to Irdeto, a leading expert on digital security, the download of pirated and unofficial downloads by 11.5% after the Covid 19 measures which was implemented. Restrictions such as lockdown and schools are closed.[7] In Russia, there were nearly 45 million views on each illegal streaming platform and more than 1.75 billion views of content and video streaming on sites such as vk.com. Though there has been a ban on these websites in Russia due to the court judgments, the other countries are running these websites and people are watching content illegally in other countries due to the lack of coordination in legal systems across the world and non-cooperation in implementing cyber laws across the world. Hence, we can see that even if a website is blocked in one country, it still causes losses as it is still active in many countries. [8] According to PETOŠEVIĆ, a network which provides intellectual property services, The European Union loses nearly 83 billion Euros, estimated tax losses of around 15 billion and loss of employment of around 400,000 every year. This shows the poor implementation of cyber laws in the countries developed or developing[9], Coming to developing countries like India, According to economic times, Nearly 20%-25% of books published in India are counterfeit, The film industry loses nearly 22,000 crore rupees and 60,000 jobs are lost due to piracy and counterfeiting. All these evidences show that there has to be efforts made to cooperate across the world in terms of legal systems to tackle the common goal of cyber security.

The shared responsibility:

We can see from the evidences stated above that it is not only the responsibility of the government but also people to act cautiously as they have to realise that establishment of a very strong judicial system that monitors over the issues of the internet as it is a much easier task to create new websites or traps that are laid to people to become victims of cybercrimes as the availability of internet, smartphones and other high technology electronic devices available to common people on a large scale. Here, it is very important that people, companies who offer digital services, government and judicial system has a role to play. The people must portray a sense of responsibility as downloads from insecure sources, unofficial resources and unpopular sites may increase the risks to cyber-attacks such as ransom wares and virus attacks. According to Malware bytes

[5] COVID-19 Exploited by Malicious Cyber Actors | CISA. (2021). Retrieved 2 March 2021, from https://us-cert.cisa.gov/ncas/alerts/aa20-099a

[6] European court of justice rules Pirate Bay is infringing copyright. (2017). Retrieved 3 March 2021, from https://www.theguardian.com/technology/2017/jun/15/pirate-bay-european-court-of-justice-rules-infringing-copyright-torrent-sites

[7] Cossack, P., & Cossack, P. (2020). Increase in Piracy During Pandemic Lockdown - Irdeto Insights. Retrieved 3 March 2021, from https://blog.irdeto.com/video-entertainment/increase-in-piracy-during-pandemic-lockdown/

[8] How covid-19 is helping online infringers to grow their business in Russia | IAM. (2021). Retrieved 3 March 2021, from https://www.iam-media.com/how-covid-19-helping-online-infringers-grow-their-business-in-russia

[9] EU Loses EUR 83 Billion Each Year in Sales Due to Counterfeiting | PETOŠEVIĆ. (2021). Retrieved 3 March 2021, from https://www.petosevic.com/resources/news/2020/08/4314

Labs, a research organisation working on challenges of risks of cyber-attacks point out that most people who are looking for pirated software and keys to access them usually are closer to risks of becoming victims of cyber attacks. [10]

As we talk about shared responsibility, Prosegur's subsidiary organisation Cipher recommends a security policy for commercial companies and businesses that have a central login system and requires a password. They recommend a strong password system to be the core principle of cyber security. They also recommend a strong training program for employees regarding the safety features of the internet space such as using secure sites, using secure passwords, providing them with the knowledge about phishing sites and how to tackle them, information on providing access to applications on their electronic devices and many others. If businesses strictly follow these measures, they will be more secure and risk free while dealing with internet spaces. [11]

On the International level there have been efforts made to tackle the cyber security issues as a measure to protect international peace and security. Many of the countries agreed on creating United Nations Convention on International Information Security to tackle the issue of cybercrime. The European Commission created the Conference on Cyber security to tackle majority issues related to cybercrimes.

Study of Legislative measures in different regions of the world:

United States of America: United States of America has been one of the oldest countries to enact robust cyber laws. They have continuously upgraded and updated the laws on cyber security. Many of the states in USA have also their own cyber laws, punishments and fines for cybercrimes. Some of the Major Cyber laws passed by the government are Cyber security Information Sharing Act of 2014 which provides information on threat to cyber security, Cyber Security Enhancement Act of 2014 which enables public private partnership to enhance cyber security, Federal Exchange Data Breach Act of 2015 which compels the organisations to inform the data breach about an individual within 60 days of the breach and finally National Cyber Security Protection Advancement Act of 2015 which enables different actors including private actors to be included in its non-federal entities.[12]

European Union: Since 2011, European Union has taken strict measures to tackle cybercrime. It has passed laws that protect children from sexual abuse, other cybercrime that threatens the security of the EU. One of the major laws that European Union has passed is also the facilitation of cross border access to evidence to investigate criminal matters. They have also established many subsidiary organisations such as the Europol which acts to fight against Cybercrime. They have also established a 'We PROTECT ALLIANCE' to fight the people who abuse children.[13]

India: India has implemented Cyber Laws in its Information and Technology ACT of 2020 where it also talks about cybercrimes and cyber security. After the amendment of 2008, It provides many different penalisation to crimes conducted. From publication of pornographic materials, to different cybercrimes such as phishing, identity theft, copyright infringement, India imposes fines up to 10,00,000 Rupees and up to 7 year imprisonment depending on the heinousness of the crime.

Protection Measures against Cyber Crimes:

[10] Arntz, P., & Arntz, P. (2020). Dubious downloads: How to check if a website and its files are malicious. Retrieved 3 March 2021, from https://blog.malwarebytes.com/how-tos-2/2020/01/dubious-downloads-how-to-check-if-a-website-and-its-files-are-malicious/

[11] Why Creating a Culture of Cyber security is a Shared Responsibility - Cipher. (2017), Retrieved 4 March 2021, from https://cipher.com/blog/why-creating-a-culture-of-cybersecurity-is-a-shared-responsibility/#:~:text=Everyone%20needs%20to%20work%20toward,maintaining%20good%20passwords%2C%20etc.)

[12] Singh, Hardeep. 2021. "A Glance At The United States Cyber Security Laws". *Appknox.Com*. https://www.appknox.com/blog/united-states-cybersecurity-laws.

[13] "Cybercrime - Migration And Home Affairs - European Commission". 2016. *Migration And Home Affairs - European Commission*, https://ec.europa.eu/home-affairs/what-we-do/policies/cybercrime_en

The Federal Bureau of Investigation clearly defines how one should protect themselves against cybercrimes. They recommend that people should be safe in the era of information and should not easily become victims of such cybercrimes. This can be used as the ideal measures to protect oneself from becoming victims to such cybercrimes. [14]

1) Protect the Password: Do not reveal or speak about passwords to sensitive information such as bank account and other digital financial account password in public. Keep it personal. It secures the people from risk of financial fraud.
2) Set Strong Password: Set difficult passwords with combination of alpha numeric and special characters so that it is difficult to crack. It will save people from becoming victims of cybercrimes.
3) Be aware of fraudulent mails and check twice before taking online services: It is better to be very careful and take precautions while taking services online. Especially anything that involves personal information and financial information. It is better to only use trusted sources and proper payment gateways to make transactions.
4) Be careful with strangers: Having pen pals, online friends and social media engagement is very common these days. It is better to be careful and make less contact with strangers on the internet. This way it becomes easier to be safe from cybercrimes and cyber-attacks. It is always good to verify if the person on the internet is legitimate before making communication.
5) Inform as well as become aware: It is very important to inform the elders, children and those who have less knowledge in accessing the Internet as they become easy victims of cybercrime.
6) Stop downloading from unofficial sources: According to Kaspersky, downloading from unofficial sources can lead to cyber-attacks such as malwares and remote access Trojans. Even if it is a little expensive, it is better to be risk free and download data from official websites and not on unofficial sources as this is the simplest form of cybercrime as well as most easy way to become a victim of cybercrime. Not only are we performing a crime by downloading infringed materials from the internet, we are also putting ourselves at risk.
7) Read official policies of institutions: Most institutions these days have anti cybercrime policies. Banks send out emails on how to be cautious if somebody contacts them regarding provision of sensitive information. Read all the measures and follow them carefully as this will reduce the risk of cybercrimes.

Conclusion

Cybercrimes have become very common these days and the people have to be very careful otherwise they become victims and may lose sensitive information such as financial information or other such information. The risk does not spare anybody, The Individual, a business, government or the military. Everybody must be aware of the situation and be vigilant towards such crimes as it causes a lot of harm to people. According to Cyber Security ventures, the world could lose nearly 10.5 trillion dollars due to cybercrimes. Hence, being vigilant and careful becomes a very important measure. It is very difficult to expect the judicial system or the government to take care of each issue as this is highly unpredictable as well as very difficult to investigate. Hence, [15]it becomes very important to study and understand the threats so that we are much safer from such crimes.

****

[14] Cyber Crime | Federal Bureau of Investigation, (2021), Retrieved 4 March 2021, from https://www.fbi.gov/investigate/cyber

[15] Cybercrime To Cost The World $10.5 Trillion Annually By 2025. (2018). Retrieved 4 March 2021, from https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/