

t
by T T

Submission date: 20-Oct-2020 11:40PM (UTC+0800)

Submission ID: 1420965886

File name: COVID-19_Pandemic_and_its_Impact_on_Cyber_Crime,,.docx (22.92K)

Word count: 1252

Character count: 7357

COVID-19 Pandemic and its Impact on Cybercrime: Reflection Paper

Name

Course

Word Count: 1100 words

COVID-19 Pandemic and its Impact on Cybercrime: Reflection Paper

Introduction

The Coronavirus pandemic has rendered the world into numerous challenges as the numbers of confirmed death and infection cases continue to rise every hour. When the epidemic is over, the impact on globalization will be severe and will last for an extended period since most of the relations between nations are cut off, and nothing is going on. Coronavirus is said to slow the growth and development of globalization socially and economically. Economically, many world leaders have detached themselves from international relations, making them operate independently since their borders are closed and there is no movement between countries (Barua, 2020).

Socially, most people in numerous countries who are poor and hopeless have provided shelter, food, and other basic needs to help them survive during this pandemic. Also, several countries have helped students continue with their studies online by providing free Wi-Fi and laptops. However, through the epidemic, the only thing left that could assist in developing trade is technology by mobile phones, computers, and laptops, among others. But they are not enough because most online businesses suffer losses because of the pandemic (Farzanegan et al., 2020). Traveling through any means from one country to another has been restricted because most countries are locked down, and services have been stopped.

Cybercrime

COVID 19 has also accelerated the practice of cybercrime around the globe. For instance, security breaches increased by 11% in 2019 compared to 2018, and 43% of the victims are small businesses. According to internet security statistics, on average, people are hacked 2244 times daily (Hawdown et al., 2020). Cybercrime also includes crime networks whereby hackers require

a collaborative network of cyber attackers to disseminate spam due to the required specialization. Cybercriminals have a low risk of being caught due to the technologies like the Dynamic Domain Name System (DDNS) and VPNs that enable cybercriminals to be hard to trace and remain anonymous. Hence, many people and organizations fall under cybercriminals' traps because they do not have advanced security or do not have enough knowledge about cybercrimes or technology. For example, many small organizations do not have the funds to continually improve their security system that keep away cyber attackers from accessing their information.

Everyday cybercrime takes place, which involves many people stealing money from people's bank accounts and companies. Many individuals who are caught are let out with a warning or go free even though they are found guilty of cybercrime. Hence, many individuals ask why it is difficult to prosecute individuals involved in cybercrime, and these are the reasons; jurisdiction, cybercrimes not being reported, and collecting legal evidence is difficult. Most individuals involved in cybercrimes are known to be located in different countries with the victims, making it almost impossible for prosecutors and the court to seek a conviction.

The Nature and Extent of the Impact.

According to an assessment done by INTERPOL, COVID 19 has highly impacted cybercrime activities, and the primary targets are significant corporations, critical infrastructure, and small businesses (INTERPOL, 2020). Since many individuals from the mentioned corporation have been working from home due to the pandemic, most cybercriminals are taking advantage of this guideline. Most staff are from different remote places, which makes their security vulnerable and easy to breach. Through hacking or breaching, they cause disruptions, generate profits through identity theft and fraud, and steal the companies' data to use them to create more profit. Through the COVID 19 lockdown, many malicious URLs and malware

incidents were connected to COVID 19. The private sectors of INTERPOL detected that many people were sent almost 910,000 spam messages, which indicated that they related to the guidelines of COVID 19. Every person who clicked on a malicious URL related to COVID 19 regulations was defrauded 100 dollars to prevent the virus from infecting people's computers, phones, and laptops that would cause loss of all data.

INTERPOL Secretary General Jürgen Stock explained that cybercrimes and cybercriminals have increased rapidly and boosted their attacks by exploiting their victim's uncertainty and fears caused by the economic and social instability formed by Corona Virus (INTERPOL, 2020). Many online phishing and scams have been reported through deploying phishing emails that impersonate health and government authorities concerning the COVID 19 regulations. Also, it has been reported that cybercriminals have been using malware that is disruptive against healthcare institutions and critical infrastructure because of financial benefit and high impact. Another impact of COVID 19 on cybercrime is data harvesting malware, in which cybercriminals use information related to COVID 19 to lure their victims whereby their data, network, and money are stolen and compromised. Therefore, the vulnerability of individuals who work from home will continue to increase cybercrime practices because cybercriminals will create more sophisticated and advanced technology used to attack their targets.

Measures put in Place to Curb Cybercrime.

Most organizations use Cybercrime to prevent the occurrence of cybercrime. For example, cybercrime surveillance can help an identity theft victim to gain access to their stolen information. The systems involved in surveillance assists individuals to track cybercriminals and provide protection to prevent other breaches and attacks. With cybercrime surveillance, security

breaches and attacks are detected early enough and provide monitoring and controlling services to the security systems to avoid any attacks that might happen in the future. Therefore, organizations and individuals are protected from malicious cyberattacks from identity theft and data destruction on computer networks. This works by identifying the dark web information, which alerts individuals and organizations of the incoming threat. It also ensures that the breached information is recovered, which prevents the victims from incurring huge losses.

Hence, the Computer Fraud and Abuse Act (CFAA) has improved the laws that prevent cybercrime in the United States. These laws have been enhanced to provide civil and criminal penalties for the attackers and charge cybercrimes (Bellia, 2016). They are also used to cater to various issues prosecuted in the court of law, such as damaging computers, password trafficking, cyber extortion, among others. Strict measures have been provided by the act to show organizations and individuals how to tackle and prevent cybercrime from affecting them. The measures taken include educating the public on methods of securing their information by the development of computer protection through strong and difficult passwords to prevent their data from being stolen or attacked by cybercriminals, especially during the COVID 19 epidemic. This will enable the public to gain knowledge on how to curb cybercrimes. Therefore, cybercriminals will have less access to the public and organization's information, which will enable the reduction of cybercrimes. The government should also chip in by providing authorities with the required resources to reduce cybercrime since it has affected many individuals and organizations during the pandemic.

References

- Barua, S. (2020). Understanding Coronanomics: The economic implications of the coronavirus (COVID-19) pandemic (No. 99693). University Library of Munich, Germany.
- Bellia, P. L. (2016). "A Code-Based Approach to Unauthorized Access Under the Computer Fraud and Abuse Act." *Geo. Wash. L. Rev.* 84: 1442.
- Farzanegan, M. R., Feizi, M., & Gholipour, H. F. (2020). Globalization and outbreak of COVID-19: An empirical analysis (No. 202018). Philipps-Universität Marburg, Faculty of Business Administration and Economics, Department of Economics (Volkswirtschaftliche Abteilung).
- Hawdon, J., Parti, K., & Dearden, T. E. (2020). Cybercrime in America amid COVID-19: the Initial Results from a Natural Experiment. *American Journal of Criminal Justice*, 1-17.
- INTERPOL. (2020). INTERPOL report shows an alarming rate of cyberattacks during COVID-19. <https://www.interpol.int/en/News-and-Events/News/2020/INTERPOL-report-shows-alarming-rate-of-cyberattacks-during-COVID-19>