Impact of Covid-19 on Cyber Security Field

Sachin Upadhyay

Department of Mathematical Sciences & Computer Applications,
Bundelkhand University, Jhansi, UP, India

Abstract:

Now a day's whole world is experiencing one of the worst pandemics of this century. The COVID-19 pandemic has had a massive impact in the world and has impact on several countries to a standstill already. During these times cyber security is of even more importance, as the environment is just right for cyber criminals to strike. In this paper we will be discussing and analyzing the impact of covid-19 on cyber security field. Society has faced a rapid increase in the cyber attacks during lockdown. This paper provides all the current trends of cyber security attacks during this pandemic and how the attacks have changed their life. The impact of COVID-19 on society, from a cyber security threats perspective is also provided and a discussion on why cyber security education is still very important and rarely known to the users.

Keywords: Cyber security, Cyber crime, Cyber Security Awareness, COVID-19, Cyber Security Education

1. Introduction:

As we know that due to COVID-19 the world will not be able to be the same as before. The year 2020 has brought along discussions about the corona virus family of viruses and how they are impacting our daily lives [1]. COVID-19 had a very bad affect on society as a whole at the start of 2020. The virus was first identified in Wuhan, Hubei China in December 2019 [2]. Subsequently, on the 11th of March 2020, the virus has been classified as a pandemic by the World Health Organization (WHO) [3]. Along with the uncontrollable amount of infections across the world, it has also brought along an era of mass psychogenic illness and collective illusions of threats. This paper is written in the mid of May 2020, that explores the impact the virus has had on the cyber security and how it is impacting the daily lives of people. It is well known that corona virus is having a massive impact in our society and governments are putting entire country in lock down in order to restrict virus from spreading in the whole country. The aim of this paper is to explore the exact impact the COVID-19 on cyber security of the world. Currently there is minimal or no awareness of cyber security in the general public on what accurate news is and what fake news is apart from experts of cyber security. There are also corporations trying to implement their own agendas or views, during these COVID-19 crisis cyber criminals are trying to profiteer out of this pandemic.This paper will be exploring what are the current impacts that the peoples are facing concerned with cyber security especially in the time of COVID-19. It also provides general guidelines on how the situation should be handled and how can we diminish the impending threats we facing. Doing analysis on the facts & figures which is currently seen and what we expect to happen within the coming months also has the advantage of reaction upon in the future in order to avoid the loss of data and money of companies and general public from cyber security hackers. Currently, the only known fact is that there is no end-goal insight for the pandemic and that the world needs to do something about it. Throughout this pandemic, it is up to the cyber security specialists to do their utmost in order to protect the general public & the services they use on cyber world. Something needs to be done about it, however, it might already be too late. As several articles in the past has mentioned, education is the key, cyber security vigilance is still massively lacking in the general public [4]. Frankly speaking I think we and any other were never prepared for the virus like corona because it seems to be very smart virus comparative to the viruses seen in human histories.

2. Cyber Security:

Cyber security describes the discipline dedicated to protecting that information and the systems used to process or store it. As the volume and sophistication of cyber attacks grow, companies and organizations, especially those that are tasked with safeguarding information relating to national security, health, or financial records, need to take steps to protect their sensitive business and personnel information. As early as March 2013, the nation's top intelligence officials cautioned that cyber attacks and digital spying are the top threat to national security, eclipsing even terrorism. Cyber security is the protection of internet-connected systems such as hardware, software and data from cyber-threats [5]. The practice is used by individuals and enterprises to protect against unauthorized access to data centers and other computerized systems. Privacy and security of the data will always be top security measures that any organization takes care. We are presently living in a world where all the information is maintained in a digital form or available on clouds. Social networking platforms provide a space where users feel safe as they interact with friends and near once. In the case of home users, cyber-criminals would continue to target social media sites to steal personal data because they are soft targets. Not only social networking but also during bank transactions a person must take all the required security measures while using the services. Cyber security is a continuously changing field, with the development of technologies that open up new avenues for cyber attacks. Additionally, even though significant security breaches are the ones that often get publicized, small organizations still have to concern themselves with security breaches, as they may often be the target of viruses and phishing. Cyber-attacks can be designed to access, delete, or extort an organization's or user's sensitive data; making cyber security vital, Medical, government, corporate and financial organizations, may all hold vital personal information on an individual. In order to protect organizations, employees and individuals, they need to use cyber security tools, training, risk

management approaches and continually update systems as technologies change and evolve. Cybercriminals continue to exploit public fear of rising corona virus cases through malware and phishing emails in the disguise of content coming from the Centers for Disease Control and Prevention (CDC) in the US and World Health Organization (WHO), says cyber security firm Kaspersky. In the APAC region, Kaspersky has detected 93 corona virus-related malware in Bangladesh, 53 in the Philippines, 40 in China, 23 in Vietnam, 22 in India and 20 in Malaysia [6]. Most probably this data must have been increased with the increased cases of corona inspected individuals.

3. Cyber Security challenges earlier and during COVID-19:

One of the most difficult parts of cyber security is the continually evolving nature of security risks. As new technologies developed & implemented in new or different ways, new paths of attack are developed as well. Keeping up with these continues changes and advancement in attacks can be challenging to organizations, as well as updating their practices & following precautions in order to protect against potential vulnerabilities. It is continually challenged by hackers, data loss, privacy, risk management, and changing cyber security strategies. Nothing currently indicates that cyber-attacks will decrease. Moreover, with the more entry points, there are for attacks, the more cyber security is needed to secure networks and devices. Now a day, there is a lot of potential data available on cyber world of an individuals or an organization gathered after using their services through any devices like mobile, computer or other smart devices, which is used by cyber criminals as per their need to steal personally identifiable information. For example, an organization that stores personally identifiable information in the cloud may be subject to a ransomware attack, and should do what they can to prevent a cloud breach [7]. Cyber security should also address end user education or awareness programs so that they may not accidently bring a virus into a working place through their devices. One more challenge to cyber security includes a job shortage. As the exponential growth in data from businesses become more important, the need for more cyber security personnel to analyze, manage and respond to incidents increases especially in the time of corona virus. It is estimated that there are two million unfilled cyber security jobs worldwide. Cyber security Ventures also estimates that by 2021, there will be up to 3.5 million unfilled cyber security jobs [8]. However, new advances in machine learning and artificial intelligence (AI) have started to be developed to help in organizing and managing data although not to the effect needed. COVID-19 has forced me, and everyone else, to become more dependent on the internet as desperate measures, such as social distancing, disrupt economic activity and everyday life due to work from home. In cyber world, dependency creates vulnerability and malicious attempts to exploit due to unplanned online social activities have naturally more profitable for the hackers. Governments and other officials reports that criminals are creating & selling fake COVID-19 cures online, posing as governmental health organizations in phishing emails, and inserting malware into online resources tracking the pandemic related activities. Due to Corona virus most of the educational organizations or Institutions are working from home to minimize the loss of academic year of the students by using different types of online meeting platforms like Zoom cloud meeting App, Webinar and Webex Meet etc in order to organize classes, webinars and conferences but hackers are active to participate in such activities to gain some private and useful information to achieve their targets. On the other hand the companies and banking organizations are worried on using online meeting platforms as it risk their customer's data and information. During lockdown we also came to know by the government the meetings held on Zoom cloud app can be risky as far as privacy of information is concerned that can be a great opportunity of the hackers.

4. Some steps for managing cyber security threats:

Although in the computer hackers story usually embellish with images of a man sitting in a dark room but, what is the biggest threat to the security of any business or organizations? Well in fact it is human psychology and ignorance, employees can often do much more damage to an organization's data integrity or who leaks information for normative reasons, or someone who sells off personal information. An attack can be as simple as somebody calling or mailing up to a person, pretending to be a colleague and asking for some confidential information's like a password or some id proof's perhaps, or customer data. This mistake of any individual or any organization's leads to a biggest security breach, as convicted hacker turned security consultant. Most of employees have practiced the things that can put their company's IT security at risk. A company can spend hundreds of thousands of rupees on firewalls, intrusion detection systems and encryption and other security equipments or techniques, but if an attacker can call one trusted person within the company and that person complies, and if the attacker gets in, then all that money spent on technology is essentially wasted. Software developers and vendors need to think that the secret to cyber security is better security technologies, but it is not only up to the security equipments or techniques used, it's up to the management of organizations to have effective training, education and risk management procedures & better implementation of policies that promote security awareness along with good communication that protect the overall security of the organization. "A recent study by Cisco found that as many as two-thirds of employees have done things that can put their company's IT security at risk — like walking away from their computer without logging off, leaving the organization with corporate data copied to their tablet, smartphone or a USB, or moving files to dropbox without permission. Leaving computer passwords in open sight [9], Losing devices like a laptop."The good news is that negligence can at least be reduced through education and communication.

5. Conclusion:

Computer security and cyber security are very broad topic that is becoming more important because the world is becoming highly interconnected with networks and their associated clouds being used to carry out critical transactions. Cyber crime continues to spread along different paths with Year by Year as it passes and so does the security of the information. The latest and disruptive technologies, along with the new cyber tools and threats that come to light each day, are challenging organizations with not only

how they secure their infrastructure, but how they require new platforms and Artificial intelligence to do so. There is no perfect solution or tool to avoid cyber crimes but we should try our level best to minimize the risk or negligence while handling, carrying and passing our important and personal information in cyber space. We and world will take years to overcome from the COVID-19 pandemic which cannot be denied. COVID-19 has brought huge negative effect, panic and confusion. All of situation had a massive impact on the mental state of individuals and the cyber security threat transformed massively, almost overnight. There was a significant increase in cyber security attacks as leaders were poised to make tough decisions on the future of their countries. Society and individuals were totally in a state of confusion of what was happening and what will happen at this time and not knowing how to react to the situation and the cyber criminals fully utilized this pandemic situation to fulfill their dreams.
The time is now to focus and take hard decisions on cyber security education, as it is right now where it is most needed. Organizations need to start investing on to buy best of the cyber tools and hire experts, as the risk to the organization has significantly increased. The internet users are no longer behind the organizations firewalls; each employee is only behind their own home router, with limited to no security. People need to be aware, however, we require organizations to educate their employees in an effort to protect themselves. Future scope of this paper is very bright because pandemic situation has shown us that the symptoms and cure from corona virus is still unknown similar in the manner that we are still unable to map the minds of cyber criminals that how they follow the internet users in future to fulfill their goals or target to harm peoples around the universe.

References:

1. World Health Organization Corona virus Accessed: 20 March 2020.
   URL: https://www:who:int/health- topics/corona virus
2. Wanda Markotter. COVID-19: Why it matters that scientists continue their search for source of ‘patient zero’s’ infection Accessed: 19 March 2020. URL: https://www:up:ac:za/news/post 2880755-covid-19-why-it-matters-that-scientists-continue-their-search-for-source-of-patient-zeros-infection-
3. World Health Organization. WHO Director-General's opening remarks at the media briefing on COVID-19 - 11 March 2020. Accessed: 20 March 2020
   URL: https://www:who:int/dg/speeches/detail/who-director-general-s-opening-remarks-at-the-media-briefing-on-covid-19---11-march-2020
4. C Hadnagy. Social Engineering The Science of Human Hacking. Publisher: Wiley.Year: 2018
5. Digitalguardian.com
6. Ciso.economictimes.indiatimes.com
7. Searchsecurity.techtarget.com
8. Masterclass.economictimes.indiatimes.com
9. www.cfr.org