A Survey on Emerging Cyber Crimes and Their Impact Worldwide

1

Suraj Gangwar
University of Delhi, India

Vinayak Narang
University of Delhi, India

INTRODUCTION

Cybercrime is an unlawful act wherein the computer is a tool or target or both. The number of cybercrimes has escalated in recent times. The opportunity for cybercrime is increasing with the increasing number of internet users. In the year 2016, it was reported as the second most commonly reported crime across the world. Report published by World Economic Forum placed cybercrime in top five of the global risk for 2018 (The Global Risks Report 2018 (13th Edition), 2018). The reason behind is simple: the rate of internet connections and the ever growing number of computer devices are outpacing our ability to properly save them (Security Predictions for 2018 Paradigm Shifts, 2017). In today's increasingly connected digital world, organisations are too hyper-connected with a new wave of technologies to improve their performance. At the same time cyber-attacks are becoming more sophisticated and impactful (Cybersecurity Regained: Preparing to Face Cyber Attacks, 2017). Embracing of technical innovations such as the Internet of Things (IoT), cloud computing and AI/ML, by organisations provides cybercriminals with new avenues for attack.

As per a report generated by Global Cyber Security Index (GCI), it can be inferred that majority of the countries in world are not yet ready to deal with cyber-attacks. GCI categorizes the countries depending upon their level of cyber security. It divides the countries in three stages

1. Leading stage: which includes countries that show high commitment to face cyber-attacks
2. Developing stage: which includes countries that are increasingly digitized but are still developing their cyber security capabilities
3. Initiating stage: which includes countries whose economies are only beginning to be digitized and where cyber security efforts are just a beginning.

The 2017 report reveals that only 21 countries are at a leading stage and 96 countries are still at the initiating stage. So there is still much needed to be done to tackle cybercrime menace efficiently (Global Cybersecurity Index (GCI), 2017).

DOI: 10.4018/978-1-5225-9715-5.ch002

BACKGROUND

The Internet connection was available to general public in 1989 and the first ever website was launched in 1991. Today, there are more than a billion websites and the number of internet users is increasing with each passing day. Figure 1 shows exponential growth of the internet users from 1995 to 2017. There will be 6 billion internet users by 2022 which equals 75 percent of the estimated world population of 8 billion. This prevalent and dominant nature of computers and interenet in our life has made cybercrimes more prominent (Morgan, 2017).

The first cyber attack took place in 1988. Morris Worm (named after its creator) infected thousands of computer systems and it took almost 72 hours to halt it. Nowadays these kinds of attack are frequent in numbers (Shackelford, 2018). The growth in importance of cyberspace across the globe has enabled vectors for, and broadens the scope of many existing forms of cyber-attacks. On one hand, cyberspace facilitates globalization of businesses and on the other, it has become a global platform for committing crimes. Individuals or more specifically cybercriminals from across the globe are using this environment to attack critical infrastructures, government and private businesses by stealing, compromising the integrity of, and destroying the data. It has created new marketplaces and even the trafficking and exploitation of human and gives a privilege for the creation and exchange of solicitation and sexual exploitation related materials (Emerging Trends In Global Cyber Crime, 2017). Cybercrimes are diverting from traditional to newly advanced crimes that can create the hoax in the world for example the Petya ransomware paralyzed the biggest container port in Mumbai,India; the cybercriminals breached the presidential election campaigns in France and USA (Cybersecurity Regained: Preparing to Face Cyber Attacks, 2017). Cybercriminals are fueled primarily by economic motives and non-economic motives. Crimes done with economic motives may include cheating, credit card fraud, money laundering, cryptojacking etc. Crimes done with non-economic motives may include cyberstalking, cyberbullying,

Figure 1. Growth of internet users from 1995 to 2017
Source:https://www.internetworldstats.com