ISSN No:-2456-2165

Increasing Rate of Cybercrime and Countermeasures Required

Rishab Gupta

Abstract:- The purpose of this research is to examine the threats cybercrimes pose to society. The concept of cybercrime is introduced and different types of cybercrimes are explored. This paper provides information about the common areas where cybercrime usually occurs. The research paper also includes the various tricks used by cybercriminals to lure people to fall into their traps. It suggests that the increased cybercrime has two primary causes:- Lack of education of people and their carelessness while using the internet like leaving personal details and credit card information on non-secure websites. It further provides data of the rapid increase of cybercrime over the past 10 years with the help of graphs and various statistics while also providing a detailed list of countries that it has affected the most and the scars it has left on them. Discussions are made from the data and the role of technology in combating such situations is explained while various other countermeasures are also suggested.

I. INTRODUCTION

The invention of the Computer has made the life of humans easier, it has been using for various purposes starting from the individual to large organizations across the globe. People are using these computers for personal benefits leaving their personal information all over these machines. This gave birth to "Cyber Crime". Cybercrime is any criminal activity that involves a computer, networked device, or network. It is argued that it is an offense committed when the computer is the main instrument of crime or when the computer is targeted for the crime. activities. Computer crime mainly consists of unauthorized access to computer systems data alteration, data destruction, theft of intellectual property. Cyber Crime in the context of national security may involve activism, traditional espionage, or information warfare and related activities. Fraud and deception aren't just a threat in real life – a range of virtual scams have been increasing significantly on the Internet for some time now. This means we have to take a new approach to evaluate possible threats. First, let us see the possible threats and the traps laid down by cybercriminals and how it has affected different countries. As many as 89% of all emails sent are so-called spam: emails you have never asked about offer you cheap credits, discounts, and a wide range of other products and services. These offers are by no means legal, and these messages often contain links to websites infected with viruses. Cybercriminals are very smart and are particularly active during major festivals such as Christmas and Easter, especially Valentine's Day. For bad guys, the latter is especially a once-in-a-lifetime opportunity-traditionally, on this day, you can admit your feelings for someone without embarrassment. Games available for download usually contain cracking tools that can be used to circumvent copy protection. These tools are provided by hackers, either because they believe that all content should be free, or because they want to make an impression on the hacker site. And download files may come with associated malware; cybercriminals know there's a big market for free content, and by disguising their malware as popular files, or adding their malware to popular files, they're increasing the number of potential victims. 2020 was challenging for everyone including companies, regulators, individuals because of the pandemic. Due to the limitations imposed by the epidemiological situation, particular categories of users and businesses were increasingly targeted by cybercriminals. In a particular Cyberattack, the hackers are targeting those in the age group of 18-44 years, for whom finding a vaccine dose is still more difficult. The link misleads the users to download an app for the vaccination registration for the 18+ age groups. But in reality, it downloads a malicious APK when the unsuspecting user clicks on the download button. The main goal of the app seems to be revenue generation by displaying ads and spreading itself through the victim's contact list and SMS. Now let us see how cybercrime has affected the world. It is estimated that the damages worldwide accrue to over 2.8 billion dollars every year. Cybercriminal activity costs the UK billions of pounds annually and according to the Cyber Security Breaches Survey 2020 almost half of businesses reported having cybersecurity breaches or attacks in the last 12 months. Overall, more than half of Internet users worldwide have experienced cybercrime. According to the survey results from November to December 2019, online users in India are most likely to be victims of cybercrime, as 80% of Indian respondents claim to have experienced cybercrime. AOL users ranked second because 61% of American respondents said they had been victims online. In the United States, most of the 1,473 data breaches each year affect businesses and medical or healthcare organizations, with 644 and 525 data breaches respectively. The survey found that in 2016, 7% of Canadian companies reported that cybercrime caused losses between US$500,000 and US$100,000. The CSIS study reveals that China and Russia have been the largest source of attacks in cyberspace since 2006. In December of 2018 alone, four major incidents were reported involving China, while three involved Russia. To stop the increase of Cyber Crime, the following measures can be taken. There have been efforts to combat cybercrime by various organizations such as the United Nations, the European Union, the Council of Europe, and Interpol. The UN adopted The

United Nations Convention against Transnational Organized Crime to fight against organized crime. We can also take some measures to prevent falling prey to cybercrime. Use a full-service Internet security suite, use strong passwords, update your software, manage your social media settings, talk to your children about the Internet, stay up to date with major security breaches, and understand where identity theft can happen. If you think you have become a victim of cybercrime, you need to notify the local police. Even if the crime seems small, this is important. Your report may assist the authorities in investigating or may help prevent criminals from using others in the future. The following graphs will give us more information on Cyber Crime.

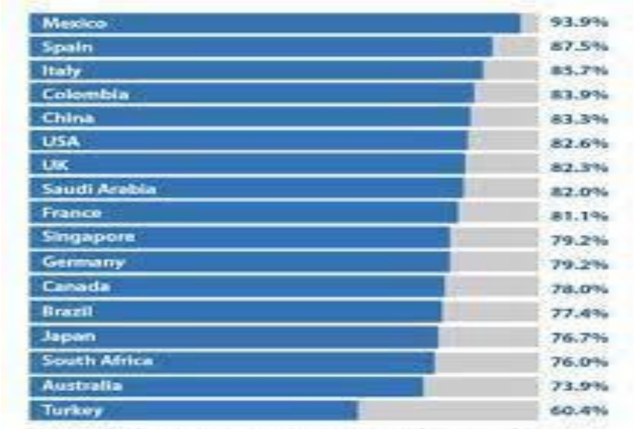
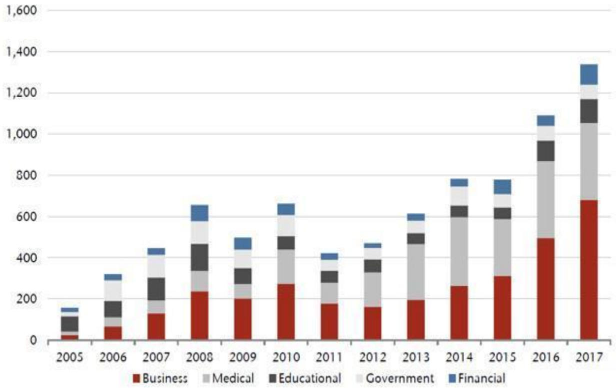
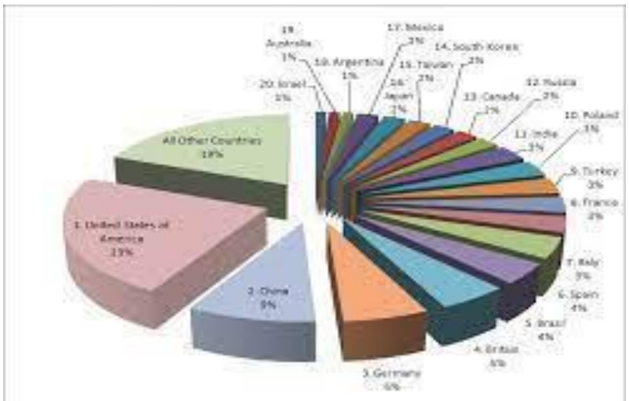
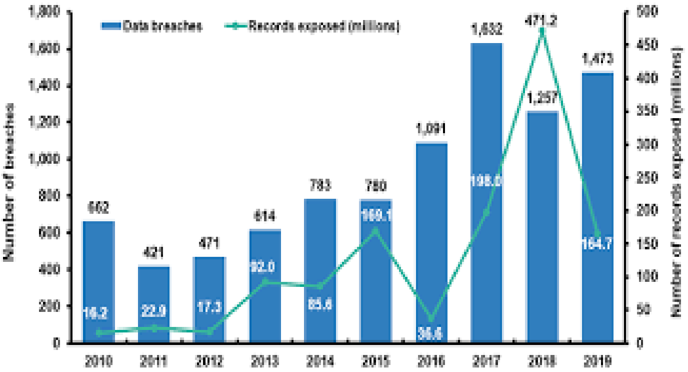


Figure 4: Percentage compromised by at least one successful attack in the past 12 months, by country.





Cybercrime: Top 20 Countries



II. ANALYSIS

The above graphs tell us about the growing rate of cybercrime in the last decade. They tell us that despite all the technology and resources available even countries like the USA have fallen prey to such an attack and no country has escaped from its trap. It also tells us about the different fields cybercrime has affected and how the number increases exponentially each year. Businesses have been the main target of cybercriminals with medicine being the second most hit profession. There have been millions of breaches that also threaten the safety of the people. The graphs inform us that we need to improve our resources and find a solution by taking stringent measures before the growing problem of cybercrime results in an international crisis.

III. MATERIAL AND METHOD

1.Method:- The study includes the different types of cyber crimes done by Cybercriminals and how they lure the users to fall into their trap. Before their inclusion, all the crimes were thoroughly studied and made sure they affected the respective organization or people. The data ranges from The Zeus Trojan virus scam in 2010 to the recent Sweepstakes scams in 2021

2.History:- A detailed history of the effects of cybercrime on the world was done and various preventive measures were suggested. The range includes information on how to combat different threats, raises awareness to prevent people from falling prey to such activities while simultaneously educating people.

3.Approach:- The data includes various graphs and statistics which further develops our knowledge about cybercrime and informs us about its various impact on different countries and the areas of business it has affected the most.

IV. CONCLUSION

The research reveals the rapidity of global cybercrime. Even large organizations with top talent and a large amount of resources dedicated to cyber security have suffered major cyber security damages. The main perpetrators of cybercrime are young people who may have the technical ability and experience to commit computer-related crimes. The paper suggests that the response to cybercrime needs to be proportional. More highly skilled workers in cybersecurity roles are necessary measures to deal with threats. People need to be educated and raise awareness so that the world is free of cybercrime.

REFERENCES

[1]. https://www.ijert.org/a-descriptive-study-on-the-impact-of-cybercrime-and-possible-measures-to-curtail-its-spread-worldwide

[2]. https://www.researchgate.net/publication/275709598_CYBER_CRIME_CHANGING_EVERYTHING_AN_EMPIRICAL_STUDY

[3]. https://core.ac.uk/download/pdf/234676934.pdf

[4]. https://www.strath.ac.uk/whystrathclyde/news/researchersannounceplansforsecuritysolutionthattrapscybercriminalsinavirtualnetwork/

[5]. https://securelist.com/financial-cyberthreats-in-2020/101638/

[6]. https://www.statista.com/statistics/290525/cyber-crime-biggest-online-data-breaches-worldwide/

[7]. https://us.norton.com/internetsecurity-how-to-how-to-recognize-and-protect-yourself-from-cybercrime.html

[8]. dannyranjeev.wordpress.com

[9]. www.garshigh.co.za

[10]. Submitted to South University

[11]. www.coursehero.com

[12]. www.statista.com

[13]. www.usnews.com