International Journal of Social Science and Economic Research

ISSN: 2455-8834

Volume:08, Issue:08 "August 2023"

'CYBER SECURITY' VERSUS 'CYBER CRIMES', AN EXPLORATORY STUDY WITH SPECIAL REFERENCE TO ITS GROWTH AND ITS IMPACT ON A COMPANY'S PROFITABILITY

Rishit Talwar

The Doon School

DOI: 10.46609/IJSSER.2023.v08i08.024 URL: https://doi.org/10.46609/IJSSER.2023.v08i08.024

Received: 20 August 2023 / Accepted: 31 August 2023 / Published: 5 September 2023

ABSTRACT

The paper has attempted to understand the increasing use of educated computer technologists in hacking into computers to extract valuable information. Companies and individuals are working round the clock to enhance cyber security so that they can foil such attempts. With the advancement of artificial intelligence, there seems to be some hope in which these security measures can be adequately enhanced and data secured.

Keywords: Cyber-security, cyber-crime, phishing, hacking, hacktivists, Artificial Intelligence, Company's profitability, financial implications

Research question: The paper will attempt to understand the growth of the importance of cyber-security in our daily lives. This technology has opened up several areas that were hitherto unheard of, but this has brought in its wake an opening for cybercrime in the economy. An analysis would be attempted concerning the positive of cyber-security versus the negative of cyber-crimes. How would this impact a company's balance sheet would also be discussed.

1. Introduction

Cybersecurity and cybercrime seem to be two sides of the same coin. Since all economies of the world are involved in liberalization and globalization the connectivity across all nations is extremely swift. This has occurred more so since the advent of the internet. In India, especially data availability and connectivity and the numerous options in cheap smartphones have further enhanced the 'oneness' of people in the country.

As this has increased, it has led to a large extent to the necessity to safeguard data in every field. With the use of computers in every sphere of our lives, the necessity to safeguard all data stored

ISSN: 2455-8834

Volume:08, Issue:08 "August 2023"

in the computer becomes imperative. Any breach of data would have disastrous circumstances for the economy, which could be in the form of government data, company data, or even an individual's personal information.

Just as the speed with which technology has progressed and storage facilities are now restricted to machines, so also has the ability of humans to use their knowledge to attack secured data. There is subsequently a race between cyber-security and cybercrime.

Figure 1: Cyber-security vs cyber-crime

Source: Google image

2. Definition:

In this day and age cyber security and cyber-crime seem to be two sides of the same coin. As technology has advanced with respect to securing of data that has been uploaded by various institutions and individuals, so has science developed where individuals, or a group of individuals have attained the knowledge to hack these accounts. There always seems to be a continuous chase between the two concepts as every time one thinks that all loopholes have been plugged, the hackers manage to circumvent it. Leading to understanding the real meaning of these terms and planning a path and taking all these factors into account for the future.

ISSN: 2455-8834

Volume:08, Issue:08 "August 2023"

2.1 Cyber-security:

Cyber-security refers to every aspect of protecting an organization and its employees in securing them against any hacking, cyber-threats, or cyber-breach. Cyber-security is basically to prevent all the stakeholders from any type of cybercrime. It is a technology that protects the confidentiality, integrity, and availability of the communication system.

Figure 2: Cyber-security

Source: Google image

Cyber-security is the practice of protecting computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks. This term can be divided into the following:

- Network Security: This means that the computer network is secured from intruders, whether they are targeted attackers or opportunistic malware(Hardware, firmware, or software that is intentionally included or inserted in a system for a harmful purpose).
- Application security: This aims at keeping software and devices free of threats. This type of security starts at the designed stage much before a program or device is deployed.
- Information security: This protects and safeguards all types of data whether in the storage form or transit.
- Operational Security: This involves accessing a network and procedures that determine how and where data could be stored or shared.

The problem arises as to how an organization reacts when there has been a breach of security. Disaster recovery policies are also in place to react to any untoward incident. Besides this, there exists End-user education that addresses the most unpredictable cyber-security factor. This continuously warns the end consumer that they should delete any suspicious email attachments.

ISSN: 2455-8834

Volume:08, Issue:08 "August 2023"

2.2 Cyber-Crime:

Figure 3: Cyber-crime

Source: Google image

Cybercrime criminal activities target and use a computer, computer network, or networked device. This crime is committed normally by hackers who want to make money, damage computers or networks for reasons other than profit(These people are known as hacktivists). Some of these hackers use the network to spread malware, illegal information, images, or any other damaging materials. At times these criminals target computers as well as infect them with a computer virus which as the name suggests spreads to other machines and networks.

A large amount of cybercrime is in the form of money-making. They include different types of profit-driven criminal activity for example, ransomware, email and internet fraud, identity fraud, and attempts to steal financial accounts, credit cards, or any other payment card information.

Since the covid pandemic, when the whole world moved to the online world, a lot of private information was stored in various types of machines and equipment. This was a hunting ground for cyber-criminals as access to this information was now easily available for professional hackers. Internet connectivity has led to an increase in the volume and pace of cybercrime activities. As the criminal need not be physically present, anonymity makes crimes such as ransomware, fraud, money laundering, bullying, and stalking much easier to commit. These activities may be carried out by individuals or groups who have little technical skill or by those who are highly skilled and have relevant experience. Criminals often choose those countries and individuals who have weak or non-existent cybercrime laws.

3. Technological cyber growth:

There has been an explosive growth of digital technologies which have created a huge amount of potential concerning security as well as conflict and cyber threats. As technology grows, its impact is felt in all spheres. Securing information has become one of the biggest challenges in today's modern world as every little item, be it in the form of bank accounts, passwords,

ISSN: 2455-8834

Volume:08, Issue:08 "August 2023"

personal information, company information, or government information, is stored in the computer. So much so that the use of paper has declined tremendously. This may be good for sustainable environmental conditions but it has left a lot of loopholes for sophisticated cyber-crimes to take place.

The business environment is changing rapidly due to technological growth which has resulted in increasing competition, as well as globalization of markets. Cashless payment systems are the norm, one notices that all of this has been made possible because of technological innovations in the fintech sector. This development has disrupted the traditional model of banking and has devised new ways in which one can access financial services and transactions.

The infrastructure which supports the above can be characterized in the following manner:

- Mobile network
- Mobile devices
- Plethora of mobile applications
- Financial technology

All of the above has been aided by:

- E-commerce
- Artificial intelligence
- Payment technologies

Data analytics has completely transformed the way finance is conducted. Fintech has played a crucial role in this integration. The greater use of finance over mobile networks has led to hackers and cybercrime increasing continuously. There is thus this connectivity with different sectors of the economy, which help each other and has resulted in the growing clan of hackers and other cyber-crime specialists.

3.1 Cyber-security:

Cyber-security is an extremely important part of information technology but securing information has become one of the biggest challenges. The moment we think about cyber-security, cybercrime comes into our minds. Despite various measures, cyber-security is a huge concern. As indicated earlier in today's world the use of physical letters does not exist anymore,

ISSN: 2455-8834

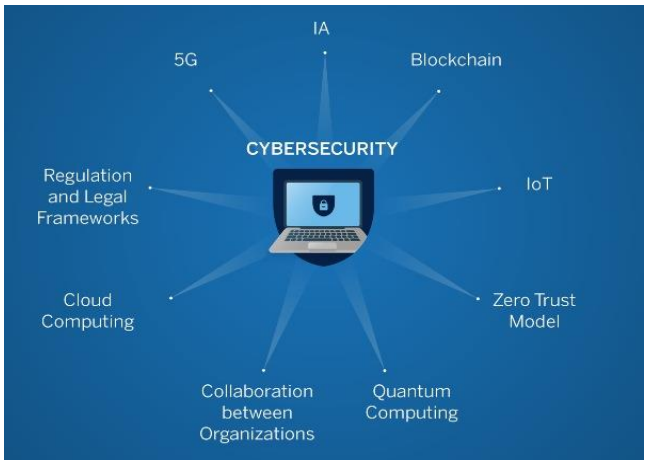
Volume:08, Issue:08 "August 2023"

the alternative is an email or an audio, or even a video. All this occurs with a click of a button. People are so happy that they are in a position to communicate with such ease, with people staying all over the world, but nobody thinks of whether the data is secured. The Internet is the biggest boon to the world and the fastest way of communication. The main issue is "effectively safeguarding private information".

Since the covid of 2019, the dependency on online modes for everything, from commercial transactions to education, etc, requires that high-quality security should exist. This system of security is not only concerning securing information, in the IT industry, but also in various other fields like cyber-space, etc.

As technology is continuously developing, the new areas of development are cloud computing, mobile computing, e-commerce, and net banking. All of the above, hold some important personal information of individuals. It is this which has to be completely secured.

Figure 4: Cyber-security



Source: Google images

Enhancing cyber-security and protecting critical information has now become the most important issue. As this is essential for a nation's security and economic well-being. The whole idea for companies and governments is to make the Internet safer. For this there are two-pronged attacks that are adopted - one is technical and the second is law agencies which have been given a free hand to investigate and prosecute cyber-crime effectively. Most governments have passed extremely strict laws to prevent any hacking of data. Besides specialists, all individuals using these facilities are continuously being made aware of how to safeguard their personal information.

ISSN: 2455-8834

Volume:08, Issue:08 "August 2023"

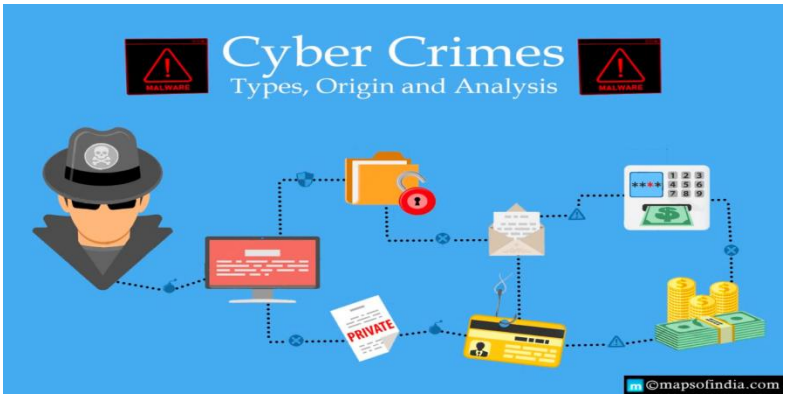
3.2 Cyber-Crime:

Cybercrime is defined as a criminal and illegal activity that uses a computer as the main means of theft. It includes any illegal activity that adopts a computer and stores evidence. The large number of cases of cybercrime has surged only due to the wider use of computers. This has happened by:

- computer viruses
- identity theft
- Stalking
- Bullying
- Terrorism

If the word cybercrime can be defined, then it means that it is a crime committed by using a computer and the internet to steal a person's identity or sell contraband or stalk victims, or even disrupt operations with malevolent programs. As the use of technology increases, the opportunity for crime automatically goes up.

Figure 5: Cyber-crime



Source: mapsofindia.com

Hackers are a set of technologists who have immense knowledge of computer technology and work for money to enter into valuable data and may sell it to any other country or rival company. Hacktivism is another form of cybercrime that is committed for political or social reasons. At times they indulge in activities like defacing a company's website or leaking personal information, maybe to send a message and create awareness for something they believe in. They

ISSN: 2455-8834

Volume:08, Issue:08 "August 2023"

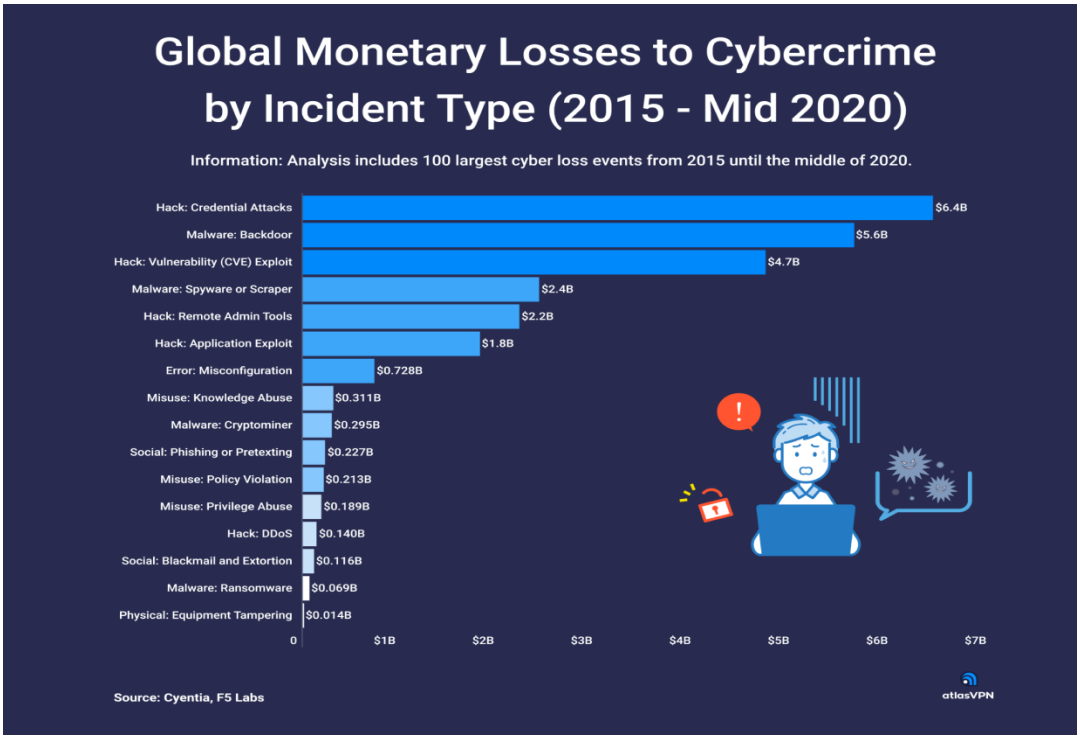
target governments, corporate, prominent organizations, religious groups, drug traffickers, and pedophiles. The moment one breaks into someone's computer, it is called hacking and if the hacking is for social activity, then at times it is called hacktivism. The difference between hackers and hacktivism is the cause or the reason why a computer is being broken into. Both of them use the same tools, but as mentioned earlier, it is the end result that is different for the two.

4. Impact of cyber-security on a company's profitability:

Cybersecurity, if looked at from the security angle and the magnitude of loss that can take place if systems are hacked would save the firm's time and cost. Firms have to take major steps in securing their profitability which means any amount of money that is spent in this sphere, justifies the cost. The impact of a cyber-attack on a business could cause:

- Financial loss (from theft of data to money)
- Loss of information
- Disruption to business (damage to reputation and damage to other companies you depend upon)

Figure 5: Global monetary losses to cybercrime by incident time (2015 - mid 2020)



Source: Cyentia, F5 labs

ISSN: 2455-8834

Volume:08, Issue:08 "August 2023"

As the world has moved more and more towards the internet and online data, it has made a large number of businesses increasingly vulnerable to cyber-thieves. The cost of cybersecurity is eventually passed down to the end consumer. Most businesses are now insured against cybercrime. What has been seen is that big companies with a huge online presence are the ones that are generally targeted. These companies are likely to be in the

- Energy sphere
- Financial services
- Manufacturing
- Technology
- Pharmaceutical sector

The cost involved for the business, if they have been attacked, would be in the form of

- Ransom
- Huge loss due to operational disruption and altered business practices
- Reputational damage is where the companies have lost control of their customers' data and have paid large amounts to settle claims.

To avoid the above, companies are willing to pay a hefty amount towards

- Cybersecurity technologies and expertise
- Notifying the affected parties of the breach of security
- Insurance premiums
- Public relations support
- Hiring lawyers and other experts

A large number of companies, to avoid cybercrime, have stopped storing customers' financial and personal information, such as credit card numbers, social security numbers, birth dates, etc.

The criminals can go to any extent and publicly proclaim and boast about the crime they have committed. This automatically results in a short-term drop in market value and decreasing

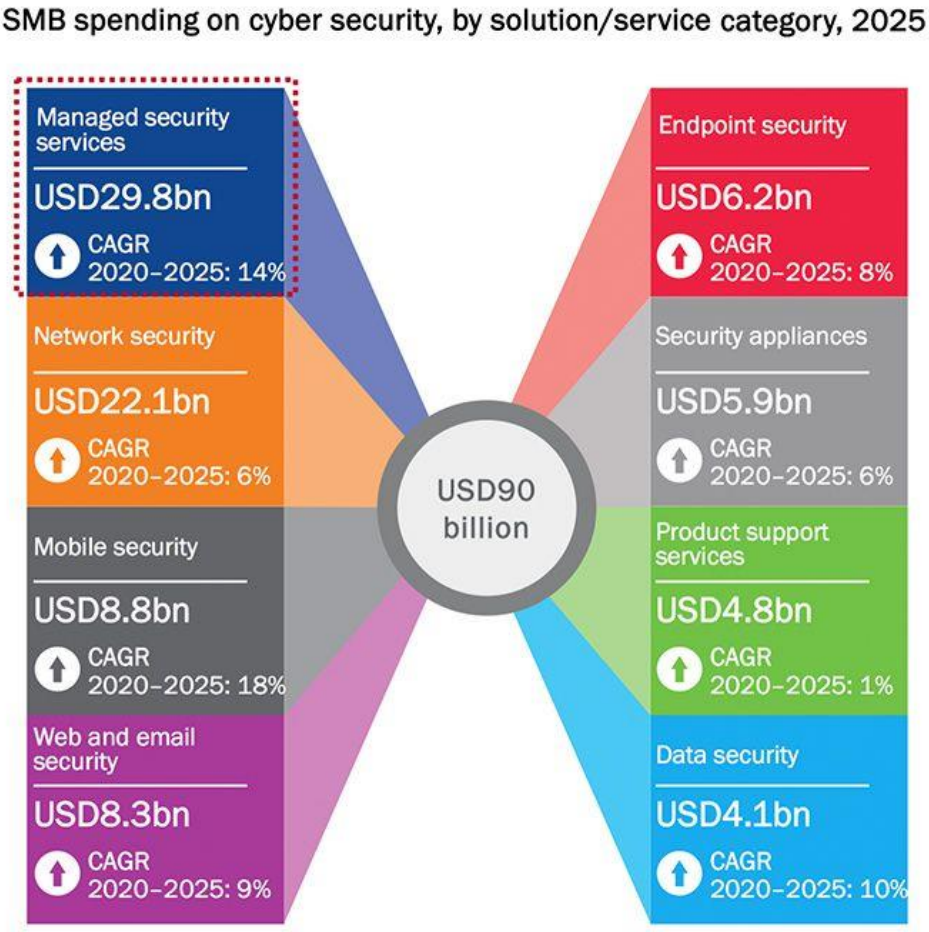
ISSN: 2455-8834

Volume:08, Issue:08 "August 2023"

revenue. Many a time, the stolen property could be from the 'cloud'. This medium could store a company's product designs, technologies, market strategies, etc. 30% of US companies have reported theft from the 'cloud' and they have blamed it squarely on their Chinese counterpart. This has happened in the last ten years.

Protecting a business from attacks is an extremely expensive proposition and can impact the relationship between a company and its customers. As cybercrime becomes more sophisticated, businesses will have to always stay one step forward.

Figure 6: SMB(Small And Midsize Businesses) spending on cybersecurity



Source: Google images

The above indicates the nuisance value that cybercrime has created the world over. The other issue that seems to be very apparent is that governments of other countries are also involved in

ISSN: 2455-8834

Volume:08, Issue:08 "August 2023"

hacking other governments' data. This means that there is huge government machinery involved in hacking.

The risk is so huge that banks can also fail due to a cyber-attack. Financial firms are three hundred times more likely to come under an attack as stated by The Boston Consulting Group. The reason is that there is a huge interconnectivity of banks and the spillover of these banks is immense. US banks are quite often susceptible to state-sponsored cyber-attacks. There was a huge spike in cyber-attacks in the early stages of the Covid-19 pandemic in 2020

5. Industry's attempt at prevention of cyber-crime:

Cybercrime requires a system of security principles that can be grouped into four key activities:

- Govern
- Protect
- Detect and
- Respond

Businesses can prevent cybercrime by:

- Encrypting all data
- Using the latest software
- Restrictions on the technicians who install software on the company's network
- Periodic depletion of software that is not used and not supported
- Knowledge of all that 'connects' to the network
- Limiting account privileges
- Using anti-virus software
- Using strong passwords. Different passwords for different accounts.
- Putting up a firewall(a security device that monitors incoming and outgoing network traffic)

All the above are important factors in what is now commonly known as 'cyber-hygiene'. The other factors that should also be taken into account are:

1. Physical Security
2. Network Security
3. Perimeter Security
4. End-Point Security
5. Application Security
6. Data Security as well as user education

ISSN: 2455-8834

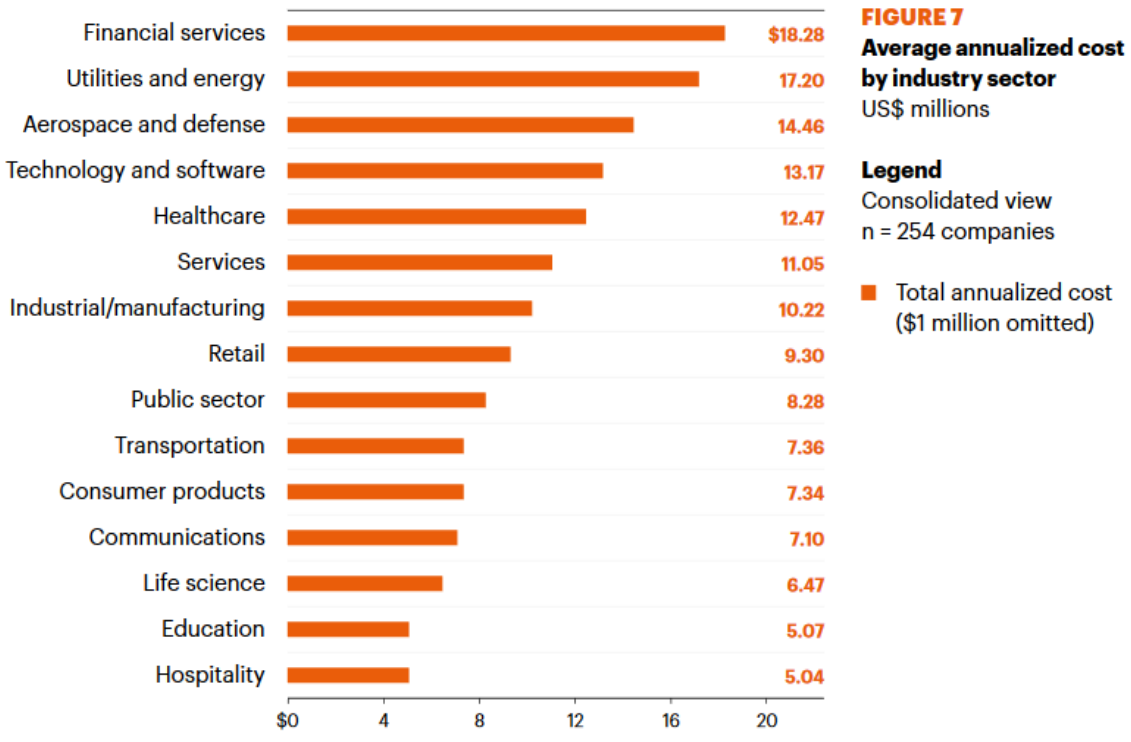
Volume:08, Issue:08 "August 2023"

The industries which are most likely to be compromised concerning cybercrimes are:

- Financial
- Health
- Intellectual
- Government Information
- Retail

The reasons for sabotage are financial gain or espionage. There are Russian State-sponsored hackers who hacked US Military and Communication infrastructure data from 2020 to 2022. The healthcare industry lost a lot of data but the main reason for the leaks was human error. In the case of financial and insurance companies, data breaches took place due to web application attacks. In such industries, there were cases of insider activity too. In the case of the education industry, the form of attack is enticing gullible students on the pretext of speaking on behalf of the company.

Figure 7: Top industries which face cyber attacks



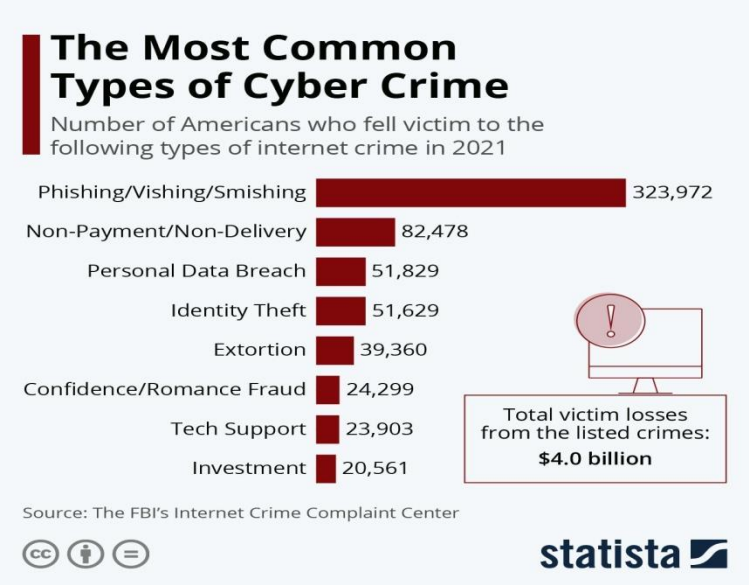
Source: Google images

ISSN: 2455-8834

Volume:08, Issue:08 "August 2023"

5.1. Most common types of cybercrime

Figure 8: Most common types of cybercrime



Source: Google images

Phishing is the most common type of cybercrime where hackers use fake emails or text messages to trick users into sharing personal information like bank details.

Malware is malicious software that damages, destroys, or exploits computers/computer systems. These could be of the following types:

- Viruses - This remains dormant till the attachment or file is opened.
- Worm - It is software that replicates itself and spreads from computer to computer. Worms can delete or change files and take up hard drive space.
- Ransomware - This is used to lock a device or steal information and the hackers demand a ransom to restore access.
- Spyware - This infiltrates the working device and monitors a person's activity.
- Trojan-horse viruses - It is software that looks legitimate but has the capability of controlling a computer.

ISSN: 2455-8834

Volume:08, Issue:08 "August 2023"

- Distributed denial of services (Ddos) attack - This means that the hacker floods the system with internet traffic resulting in slowing down of the system, inability to open files, reduced internet speed, and inability to access websites.

6. Government's endeavor to control cyber-crime

The Indian Governments' information technology act 2000 provides stringent punishment for committing various categories of cyber crimes. The Indian Government has a Cyber Crime Coordination Center Scheme. The Government has provided an outlet of rupee 400 crores to act as a nodal point in the fight against cybercrime. Encourage Research and Development activities in collaboration with academia and research institutes in developing new technologies to counter cybercrime. This nodal agency could suggest amendments in cyber laws to keep pace with fast-changing technologies, and coordination with other countries to collectively fight against cybercrime attacks.

The government has opened up various cyber crime police stations where the common man can complain and get redressal of his complaint. The institution of critical infrastructure protection as well as a national incident response and recovery plan are being actively encouraged by the government.

The extent of incidents of cybercrime has increased exponentially during the covid 19 pandemic as almost all activities were shifted to online mode. In response to the increasing number of crimes that occurred, various programs were initiated by the government of India to prevent and forewarn its citizens of the dangers of such attacks. Increasing awareness through advertising is an extremely important tool that the government has used effectively amongst its citizens on the modus operandi of potential hackers.

7. Conclusion

Cyber-crime has been on the rise and there seems to be a cat-and-mouse game played by various companies in enhancing cyber-security to catch up to the methods that hackers use in entering a computer. With the advancement of Artificial Intelligence(AI), both these sets of technologists are trying their very best to safeguard and protect their interests. With the world moving towards digitalization, there is a lot of important data and information which is stored in the computer/laptop/phone. With superior technology across all spheres, life has become impossible without the aid of these important systems. As dependence on them increases, so does the vulnerability concerning data being hacked and/or phished. This is not only for big conglomerates but also innocent individuals. The governments have set up specific cyber-crime police stations, as well as advertised widely on television/radio/newspapers on the dangers of

ISSN: 2455-8834

Volume:08, Issue:08 "August 2023"

hacking. Every individual needs to safeguard their data on their own to prevent them from becoming targets for criminal activity.

Bibliography

1. Á. Kemendi, P. Michelberger and A. Mesjasz-Lech. "ICT security in businesses - efficiency analysis". Journal of Entrepreneurship and Sustainability Issues. vol. 9. no. 1. pp. 123-149. Sep. 2021. 10.9770/jesi.2021.9.1(8).
2. Alansari, M. (2016). On Cyber Crimes and Cyber Security. *Research Gate*.
3. M. Aljuhami and D. M. Bamasoud. "Cyber Threat Intelligence in Risk Management". Jan. 2021.
4. J. O. Oyelami and A. M. Kassim. "Cyber Security Defence Policies: A Proposed Guidelines for Organisations Cyber Security Practices". Jan. 2020.
5. K. A. Memon et al.. "Analyzing distributed denial of service attacks in cloud computing towards the Pakistan information technology industry". Indian Journal of Science and Technology. vol. 13. no. 29. pp. 2062-2072. Aug. 2020. 10.17485/ijst/v13i29.1040.
6. K. Veena, K. Meena, Y. Teekaraman and A. Radhakrishnan. " C SVM Classification and KNN Techniques for Cyber Crime Detection". Wireless Communications and Mobile Computing. vol. 2022. pp. 1-9. Jan. 2022. 10.1155/2022/3640017.
7. M. Babič and D. Purković. "A new Systemic Taxonomy of Cyber Criminal activity". Jun. 2020.
8. O. T. Suryati and A. Budiono. "Impact Analysis of Malware Based on Call Network API With Heuristic Detection Method". International Journal of Advances in Data and Information Systems. vol. 1. no. 1. pp. 1-8. Apr. 2020. 10.25008/ijadis.v1i1.176.
9. R. Sardar and T. Anees. "Web of Things: Security Challenges and Mechanisms". Ieee Access. vol. 9. pp. 31695-31711. Jan. 2021. 10.1109/access.2021.3057655.
10. S. S. Alsemairi. "The Role of Digital Technologies in Combating Cyber-Trafficking in Persons Crimes". Dec. 2022.

