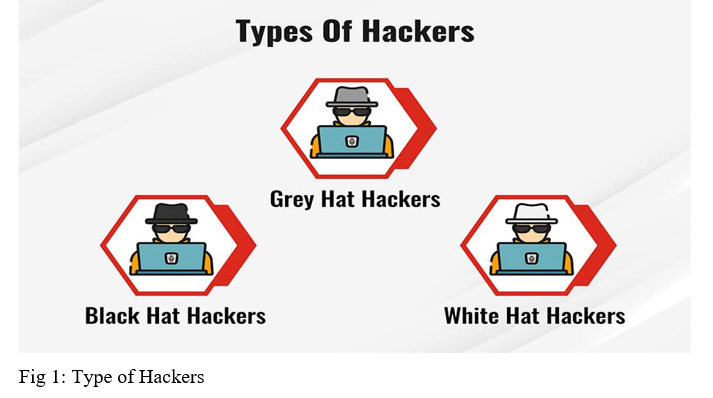
**1.INTRODUCTION**

2020 was an year of turnarounds for entire humankind as well as for the world of internet. The very little things which we never thought will automate has now become completely automated. And as a matter of fact, the relevance of cyber security measures has also now a topic of discussion. While discussing about cyber security, security breaches should also be considered. Covid-19 has paved the way for vast digitalization which we thought will occur only after several years from now. As a result, data transferring through online platforms has increased multiple times. But did we ever thought how securely our data being transmitted or sent to the other person safely without any leakage of information? The answer lies in cyber security. As the automation of services increased the number of cyber-attacks has also increased proportionally. The data breach reports on various sectors were reported frequently in global as well as local medias. The patterns and methodologies used by hackers/attackers has also advanced and many of the organizations with complicated firewalls has compromised by these anonymous individuals. It’s now become inevitable to protect the data and to secure them in this highly cyber infiltrated era.

Cybersecurity threats are estimated to cost the world US $6 trillion a year by 2021, and the number of attacks has increased five-fold after COVID-19[1]. The modern cyberattacks like DoS and DDoS attacks, MITM attacks, Phishing attacks, DNS Spoofing attacks has evolved during the time of pandemic and they have caused much more damage than their earlier interventions. Prevention and Counter Measures are the most important things that must be implemented in order to prevent these kind of data breaches and attacks. Prevention, Detection and Reaction are the 3 steps might help us guard against these attacks. Using the service of Certified personals who can perform Pen Testing on the databases can be a very effectful method. This paper is focused on pointing out the major reasons of increased cyber attacks in pandemic era. The intention is to light on the weaknesses and imbalances of current system and to provide a permanent solution for keeping the data secured.

**2.CYBER SECURITY AND CYBER ATTACKS**

The highly automated cyber world has now come to an extend that the number of cyber attacks and security issues has increased exponentially. The term cyber security can be defined as the practises and measures used for defending the computers, servers, networks, mobile devices and data from malicious individuals or attacks. It covers certain aspects like Network security, Application security and Information security. The scale of cyber threats has now multiplied exponentially especially after the Covid-19 outbreak. The pandemic has itself acted as a catalyst to the automation which was happening at a medium pace. Usual methodologies that we used in early days are now outdated in front of this highly skilled attackers /hackers. The name hacker refers to the personals who performs or launches attacks. Hacking is the act of corrupting or breaching into a system and gaining access to the data without authorization. A hacking definition is the act of compromising digital devices and networks through unauthorized access to an account or computer system. Hacking is not always a malicious act, but it is most commonly associated with illegal activity and data theft by cyber criminals.[2] A hacker is an individual who uses computer, networking or other skills to overcome a technical problem. The term also may refer to anyone who uses their abilities to gain unauthorized access to systems or networks in order to commit crimes. A hacker may, for example, steal information to hurt people via identity theft or bring down a system and, often, hold it hostage in order to collect a ransom.[3] These hackers can be further classified into 3 types.



**2.1 Types Of Hackers**

* White Hat Hackers
* Black Hat Hackers
* Grey Hat Hackers

**2.1.1 White Hat Hackers:** They are the good guys of hacking and they tries to protect the data from the attempts of the black hats using their own methods but in an authorized manner.They uses their technical skills to break into systems and check the security level to prevent from future attacks.

**2.1.2 Black Hat Hacker**s: They can be called as the bad guys in hacking. They finds out vulnerabilities and exploits them to gain access to the target and uses them for financial gain and malicious purposes, for gaining reputation etc

**2.1.3 Grey Hat Hackers:**They sits in between white and black hat hackers. Unlike black hat hackers they doesn’t use their skills to gain money or other personal benefits. They do breaks the rules and violates standard principles but they can be used for good purposes as well.

**2.2 Cyber Attack Tools**

The recent developments in cyberworld has created the opportunity for these hackers and organizations to exploit and steal as much data as they want and use it for malicious purpose. They uses hacking tools in order to create backdoors and to exploit vulnerabilities in a system and later takes advantage of it. Some of the most commonly used hacking tools are.

* NMAP
* WIRESHARK
* METASPLOIT
* BURP SUITE
* THC HYDRA

**NMAP**

It is said to be one of the best tool used to scan a network in order to find the ports that are open. It is utilized in the foot printing segment to examine the ports of the remote workstation for situating out ports is open.[8]

**WIRESHARK**

It can be called as a packet analyser. It catches all the network movements, it breaks down for succulent data like usernames and passwords in order to perform network investigating .[8]

**METASPLOIT**

It is the most commonly used penetration testing package. It comes with thousands of payloads and that can be used to exploit the vulnerabilities. It’s the best toolkit that can be used to hack into a computer.

**BURP SUITE**

An integrated platform and graphical tool for checking the security of web applications. It is a set of tools which tests and finds out vulnerabilities of a web application.

**THC HYDRA**

It is commonly used by penetration testers , it is a set of tools that can be used to generate wordlists for brute force attacks.

The modern cyberattacks will be the product of this tools and some of them can be highly destructive.

**3. CYBER ATTACKS**

A cyberattack is a malicious and deliberate attempt by an individual or organization to breach the information system of another individual or organization. Usually, the attacker seeks some type of benefit from disrupting the victim’s network. There are a wide range of cyber attacks classified depending on the threat level and nature. Six of the most common attacks are shown in the figure.

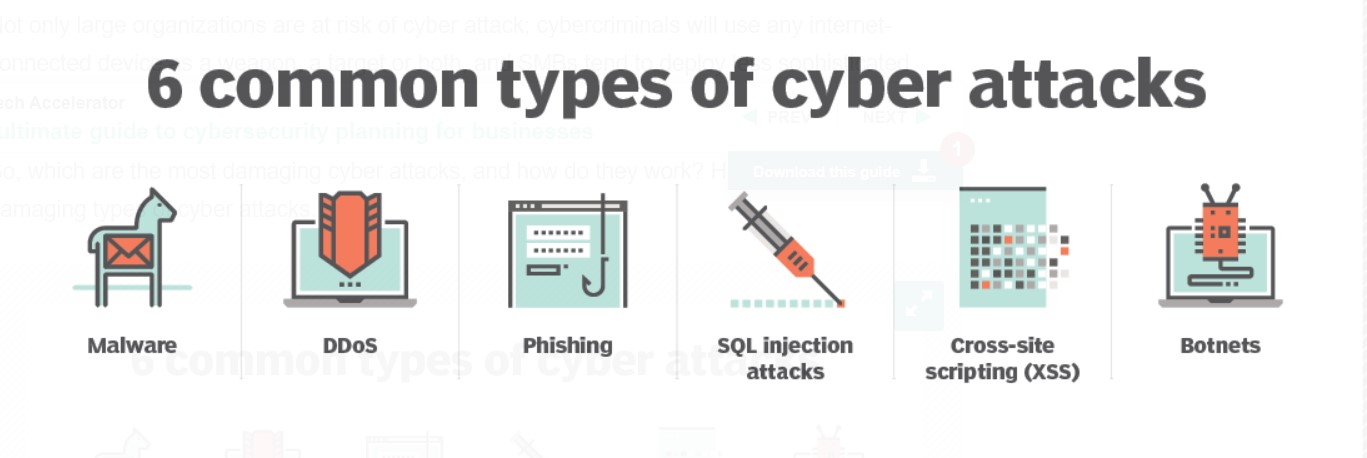


Fig 2: 6 common Cyber attacks

**3.1 Malware**

Malware, or malicious software, is an umbrella term used to refer to a hostile or intrusive program or file that is designed to exploit devices at the expense of the user and to the benefit of the attacker. There are various types of malware,

* **Ransomware:** Currently, the most feared form of malware is ransomware -- a program designed to encrypt a victim's files and then demand a ransom in order to receive the decryption key.
* **Trojan:** A Trojan horse is a program downloaded and installed on a computer that appears harmless but is, in fact, malicious. Typically, this malware is hidden in an innocent-looking email attachment or free download. When the user clicks on the email attachment or downloads the free program, the hidden malware is transferred to the user's computing device.

**3.2 DDoS**

A distributed denial-of-service (DDoS) attack is an attack in which multiple compromised computer systems attack a target, such as a server, website or other network resource, and cause a denial of service for users of the targeted resource. The flood of incoming messages, connection requests or malformed packets to the target system forces it to slow down or even crash and shut down, thereby denying service to legitimate users or systems.

* 1. **Phishing**

A phishing attack is a form of fraud in which an attacker masquerades as a reputable entity, such as a bank, tax department, or person in email or in other forms of communication, to distribute malicious links or attachments to trick an unsuspecting victim into handing over valuable information, such as passwords, credit card details, intellectual property and so on. It is easy to launch a phishing campaign, and they are surprisingly effective.

* 1. **SQL Injection Attacks**

Any website that is database-driven -- and that is the majority of websites -- is susceptible to SQL injection attacks. An SQL query is a request for some action to be performed on a database, and a carefully constructed malicious request can create, modify or delete the data stored in the database, as well as read and extract data such as intellectual property, personal information of customers, administrative credentials or private business details.

* 1. **XSS**

This is another type of injection attack in which an attacker injects data, such as a malicious script, into content from otherwise trusted websites. Cross-site scripting (XSS) attacks can occur when an untrusted source is allowed to inject its own code into a web application and that malicious code is included with dynamic content delivered to a victim's browser. This allows an attacker to execute malicious scripts written in various languages.

* 1. **Botnets**

A botnet comprises a collection of internet-connected computers and devices that are infected and controlled remotely by cybercriminals. They are often used to send email spam, engage in click fraud campaigns, and generate malicious traffic for DDoS attacks. The objective for creating a botnet is to infect as many connected devices as possible and to use the computing power and resources of those devices to automate and magnify the malicious activities. IoT botnet threats were one of the fastest growing categories of threats out there.

**4. PANDEMIC AND CYBER ATTACKS**

**4.1 Pandemic As a Catalyst**

According to the World Health Organization (WHO), the number of cyberattacks launched has increased five-fold during the COVID-19 pandemic [4]. A similar phenomenon was seen in 2005 after Hurricane Katrina, where thousands of fraudulent websites appeared soliciting fake donations and offering false government relief [5]. The occurrence of this global pandemic outbreak has acted as a catalyst for the cyber-attacks. These references proves certain situations are always taken advantage by the hackers. Studies shows that many reputed organizations were attacked by certain organizations of hackers during this post pandemic period and the origin of some of them still puzzles the authorities. Cybercriminals are developing and boosting their attacks at an alarming pace, exploiting the fear and uncertainty caused by the unstable social and economic situation created by COVID-19*.* Jürgen Stock, INTERPOL Secretary General.[6]

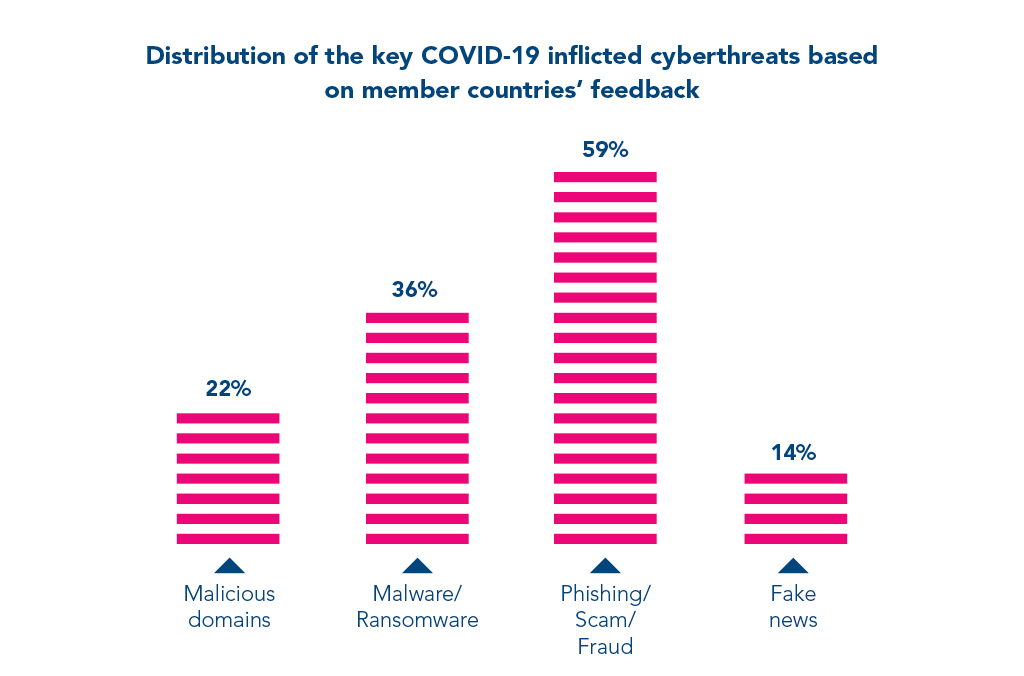


Fig 3: Surge in cyberthreats after Covid-19[6]

Many studies shows that there is almost an 81 % increase in the amount of cyberattacks in last couple of years. Even if mainstream companies are implementing prevention methods the others are not at all giving importance to the aspect of data security in their firm. The following figure shows the percentage of organizations that carried out certain activities to detect and prevent cyberattacks last year.[7]

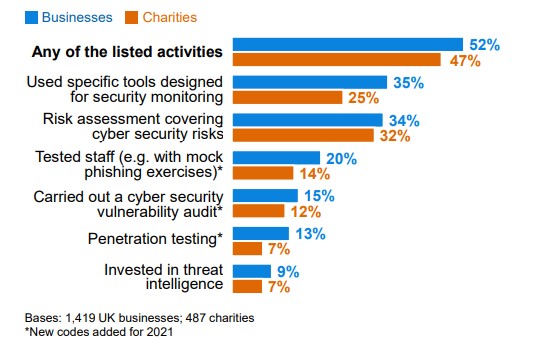


Fig 4: Percentage of organizations acted on detecting and preventing cyberattacks.[7]

• 52 per cent of large businesses and 23 per cent of high-income charities carry out penetration testing. [7]

• 49 per cent and 37 per cent respectively have tested their staff response, with mock phishing or similar exercises.[7]

• 48 per cent and 26 per cent respectively undertake cyber security vulnerability audits.[7]

All this means that the rest of the companies are not concerned about the cyberattacks and data breaches, surprisingly many of these companies are yet to detect the threats and attacks that they might get exposed to. Relatively a small amount of companies are well aware and equipped about the cyber threats around. The figure above shows the possible preventive measures adopted by the companies accordingly. The data mentioned is on UK based businesses and Veronis which is a data security and analytical company has disclosed that 64% of the Americans hasn’t checked whether they are affected by a breach or not. Their surveys showed that in the event of a data breach, 56% of Americans wouldn’t know the steps to take in response. Means only 44% are able to act against a data breach[9]. This could be even lower in other countries.

**5. CYBER THREATS IN VARIOUS FIELDS AFTER**

**COVID-19**

As discussed, the cyberattacks during the pandemic has changed many industries and its flow of work to be precise. The pandemic has caused a drastic digitalization which was not at all proper and systematic. Various fields and its operations were digitalized and the data left wide open for the attackers to take on. The world is far more connected than compared to previous times. Some of the sectors affected by this post pandemic cyberattacks are,

* Medical Industry
* Banking and Financial Services
* Educational Institutes

Cyber Security Report 2021 by Checkpoint shows whooping surge in the cyberattacks exploiting the product vulnerabilities. Citix attacks went up by a whopping 2,066% by the mean time VPN attacks and RDP attacks surged by 610% and 85% respectively[10].

**5.1 Medical Industry**

The digitalization in medical industry was the most vital thing happened during the time and it is not surprising to know that it was medical industry who suffered the most by cyberattacks. The stolen data includes data related to Vaccine development and modelling. One important factor is that medical industry depends on IOT more than any other sectors. Nowadays this IOT devices are vulnerable and they are being easily exploitable. The attacks could shut down devices or whole server networks demanding ransom to decrypt the encryption. Since mostly every medical device is connected hackers can easily get into devices like cardiac pacemakers and other lifesaving devices.[11] Even World Health Organization(WHO) were attacked by hackers in 2020 by creating a malicious site mimicking the WHO mail system to steal the passwords and user id of the employees.[11].

The existing medical database system generally adopts user connection information and simple encryption to prevent illegal users from accessing database passwords. However, in C/S mode, the client still has a username and password to access the database, and these identifiers can be simply cracked or maliciously changed. Although the circulation and sharing of information is a big risk, a lack of authentication will lead to data risks.

The below figure shows the classification of vulnerabilities in cyber security in medical industry.

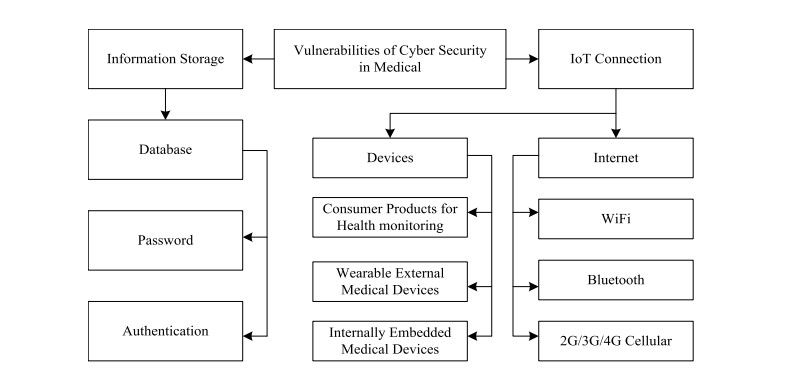


Fig 5: Cyber security vulnerabilities in Medical Industry[21].

**5.2 Banking and Financial Services**

Covid-19 has created the revolutionary working practice called work from home and in financial sector also this trend has been reflected. Its said to be the new normal in working and it has caused a huge surge in the amount of online transactions and interactions related to the same sector. Usage of technologies like RDP and VPN has increased by 41% and 33% respectively, in just two months of the Covid-19 outbreak.[12] And it must have spiked after that. All mainstream banks and financial institutions has developed online banking applications as well as other transaction gateways during the time to complete their banking transactions. Basic attacks like MITB, Phishing, DDoS attacks have taken its new form and they have caused severe damage to the services of this sector. A mass migration of workers of financial institutions to work from home has made them more vulnerable. The financial sector has been hit relatively more often by cyber attacks than most other sectors since the pandemic started. Data on attacks can be obtained from Advisen, a for-profit organisation that collects information from reliable and publicly verifiable sources (mostly in the United States), covering date, actor, loss amount and other features. There is a strong link between the prevalence of WFH arrangements – as measured by the WFH index by sector from Dingel and Neiman (2020) – and the incidence of cyber attacks between the end of February and June 2020.Outside the health sector, the financial sector

has the largest share of cyber events classified as Covid-19-related in recent months. Examples are phishing attacks that explicitly use the uncertainty around Covid-19 to entice users to open fraudulent attachments or grant attackers access to networks.

The following figure shows the surge of cyberattacks in financial sectors (Health sector excluded).

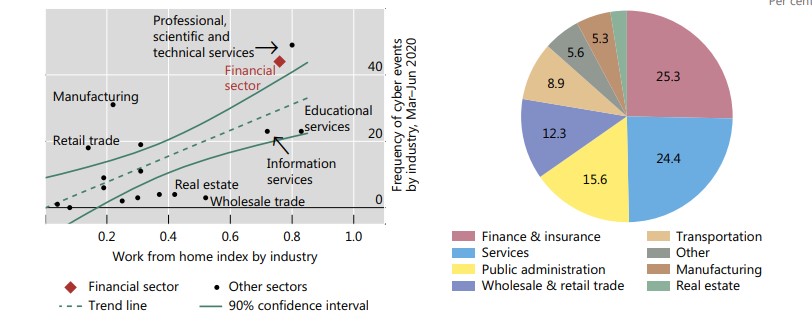


Fig 6: Increase of cyberattacks in financial industry during Covid-19 (work from home scenario)

**5.3 Educational Institutes**

The educational institutes were not a well known target to the cyberattacks but the situation has changed over the past few years. Ransomware attacks became more frequent on educational sector. Number of ransomware attacks on the educational platforms has increased during the Covid-19 when the employees and the students started to work and learn from home. Being more connected than ever before, the school systems have been especially vulnerable to cyber attacks during the pandemic time. The platforms like Google Classroom, Zoom, Duo was widely used by the institution to conduct meetings as well as teaching sessions. Times of India says quoting a report that India is the biggest target of cyber threats to educational sectors followed by USA,UK.[13] The report also shows that 58% of the attacks detected in Asia and pacific were targeted on Indian or India based educational institutions and online platforms. The victims includes Byju’s ,IIM Kozhikode and Tamilnadu Directorate of Technical Education.[13]

**6. DETECTION AND PREVENTION MECHANISMS**

Detecting a cyber attack and reacting to it as soon as possible is the most important thing that someone could do to keep the attackers and attacks at the bay. This is a part of cyber defence and it is a practice that needs to be followed on a regular basis. Analysing the various threats, Information and Communication Technology industry was forced to work more on possible countermeasures. The NATO Cooperative Cyber Defence Centre of Excellence has defined the term ‘cyber defence’ as “a proactive measure for detecting or obtaining information as to a cyber intrusion, cyber attack, or impending cyber operation or for determining the origin of an operation that involves launching a preemptive, preventive, or cyber counter-operation against the source”[15]*.*

**6.1 Detection**

On the assumption that every system is vulnerable or will be in future, it is the detection phase which is responsible for the identification and detection of any possible malware attacks or threats. Any detected malware and other suspicious activities will be reported to the administrator or will be collected using a Security Information and Event Management (SIEM) system.

**Detection Techniques**

The cyber crimes can be detected using many techniques. They can be classified into Statistical, Machine Learning, Data Mining[16].

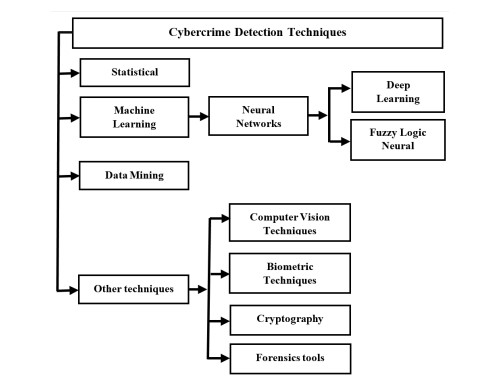


Fig 7: Classification of Cybercrime Detection Techniques[16].

The most commonly used will be discussed here.

* **Using an Intrusion Detection System (IDS)**

IDS are widely used to detect the malwares and any attempt of intrusion. There is a wide range of IDS which are classified into two based on the features where the detection sensor or entity is placed and what detection method is used.

IDS based on placement of detection entity: Network IDS, Host-based IDS.

IDS based on detection method used: Signature-based IDS, Anomaly-based IDS.

* **Using Machine Learning (ML)**

Machine Learning is the process of predicting outputs based on the given input data. The data can be either supervised or unsupervised. Machine Learning is now used to detect the cyberattacks, they uses the ML algorithms like K-Nearest Neighbor (KNN) , Naïve Bayes Classifier, Levenshtein Algorithm etc. Many researchers and developers are currently looking into the endless possibilities of ML that could contribute to the detection of cyberattacks.

* **The other techniques**

The cyberattack detection using other techniques includes the usage of Cryptography, Biometrics, Cyber Forensic tools etc.

**6.2 Prevention**

This is the phase of cyber defence which is supposed to be continuously monitoring the system in order to find any existing vulnerabilities or misconfiguration. If any thing is found against the configuration and security policies, necessary actions will be taken to patch the detected vulnerability. Many techniques and methodologies are used to prevent cyber attacks ,the commonly used ones are

* **Usage of Firewalls**

Firewalls are widely used in every systems in order to prevent any possible visit to a malicious site. In some instance we might turn the firewall of the system off, on certain occasions there is a possibility of forgetting to turn the firewall back on. This will be utilized by the hackers to use phishing and spoofing attacks.

* **Intrusion Prevention Systems (IPSs)**

Using IPSs are so crucial. Their major advantage is that they analyses the traffic flow of a network and will automatically take actions to prevent attacks in networks.

* **Access Control Systems (ACS)**

They are used to mange the privileges given to a user by the administrator over the access of user to specific data inside a particular organization. It limits the area of access of the users of several levels and if anyone tries to override their permissions then it will be taken care of.

* **Penetration Testing**

This could be the most effective and reliable technique to prevent the cyberattacks. Even though it is not used often pen-testing still remains the best option. Since cyber attacks are evolving so fast it increases the necessity of performing comprehensive pen-testing regularly to keep the data safe. There is always a possibility that even with the best up to date security measures they might result in vulnerabilities in later future. That is why we strongly insists to perform penetration testing regularly. This test must be done frequently including the testing of operating system, hardware, networks and even the pen-tester might check the behavior of the employees[17].

Notable Attacks Occurred During Pandemic Period.

* Data of more than 530 million Facebook users, including their names, Facebook IDs, dates of birth, and relationship status, was published online in April 2021[18].
* Dating app MeetMindful suffered a cybersecurity attack in January 2021, resulting in data of more than 2 million users being stolen and leaked. The hacking group behind the event managed to steal information like users’ full names and Facebook account tokens[18].
* One of the most damaging recent cyberattacks was a Microsoft Exchange server compromise that resulted in several zero-day vulnerabilities. ProxyLogon and initially launched by the hacking group called Hafnium, were first spotted by Microsoft in January and rectified in March.[18]

**7. RECOMMENDED SOLUTION**

**7.1 Ethical Hacking & Penetration Testing**

The term ethical hacking should be treated with huge importance in current scenario. It’s a widely used but commonly misused word to be precise. In fact the ethical hackers (white hat hackers) are the good fellows of the cyber world. They are very helpful, intelligent and of great usages. They are the penetration testers whom are widely now being used to secure the data and to prevent from attacks. They uses the same tools, techniques and highly sophisticated processes that the black hats who are the bad guys or the actual hackers in the cyber world. The difference is that ethical hacking is legal by all means.

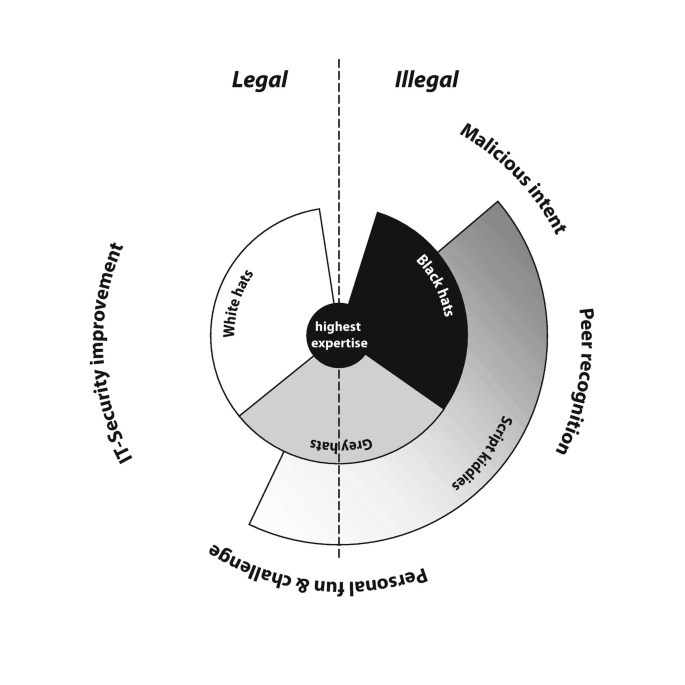


Fig 8: Ethical Hackers vs Unethical Hackers (black,white&grey hats)[18]

There are highly qualified ethical hackers who could really help with the currently ongoing pandemic scenario. Certain ethical hacking programs has now started in order to prevent the hackers from getting away in the race.

Last year Indian Express reported that a student of 10th class from Odia was praised by Liberian Government for helping them to nab a malicious hacker who got into the official website of their Finance Minister.[19]

Likely many of the ethical hackers are helping the companies and governments to detect and prevent cyberattacks. The Covid-19 has created a social economic scenario that the drastic digitalization in sectors like Medical, Banking, Educational etc. has opened the doors for hackers to do whatever they want.

Mainstream companies such as Tesla, IBM, Lenovo, Google etc. are now hiring ethical hackers following the tremors that the pandemic has created in the cyber world. Following the footprints several IT companies are also hiring the same. Even though the data of the educational institutions which is kept under direct risk of the management itself are still vulnerable. These institutions have Data Base Managers (DBMs) but very small percentage of institutions are conducting proper penetration testing on a regular basis. To stop a hacker, one needs to think like one and this is the principle that ethical hackers works on.

Why should every companies consider hiring ethical hackers.?

* To build a computer system that prevents hackers’ access and safeguard system and information from malicious attack
* To manage adequate preventive measures in order to avoid security breaches
* To safeguard user or customer information available in business transactions and visits
* To test networks at regular intervals
* To create security awareness at all levels in a business.

**8. CONCLUSION**

This paper outlines why cyberattacks have been particularly problematic during COVID-19. It has affected almost all sectors across the world . Year-over-year results indicate a fast start to data breaches in 2022 after a record-setting 2021, as more than 90% of data breaches are cyberattack-related, the Identity Theft Resource Center found. For the third consecutive year, data breaches increased when compared to Q1 of the previous year. Despite the data breach increase, the number of victims (20.7 million) decreased 50% compared to Q1 2021 and dropped 41% compared to Q4 2021. This is definitely because of the preventive measures taken by the victims over the past 2 years. In other words we can say that they have learned from their mistakes. As the co founder of EC council Jay Bavisi says we do definitely need ethical hackers now more than ever in history. This paper has covered several aspects of cyber threats and some statistics that underlines his statement. Certified ethical hackers can be an effective solution on the present scenario against the cyber criminals as well as they are a shield against the cyber threats that could make your data in danger. We have talked about the several advantages of using ethical hackers (Pen-testers) to secure the business. They are what the current society demands.

# 

# REFERENCES

* + 1. Williams, C. M., Chaturvedi, R., & Chakravarthy, K. (2020). Cybersecurity risks in a pandemic. Journal of medical Internet research, 22(9), e23692.
    2. What is hacking, Types of hacking and more url: <https://www.fortinet.com/resources/cyberglossary/what-is-hacking>
    3. TechTarget Definition of Hacker url: <https://www.techtarget.com/searchsecurity/definition/hacker>
    4. WHO reports fivefold increase in cyber attacks, urges vigilance. World Health Organization. 2020 Apr 23. URL :https://www.who.int/news-room/detail/23-04-2020-who-reports-fivefold-increase-in-cyber-attacks-urges-vigilance
    5. Hurricane Katrina fraud. FBI. URL: <https://www.fbi.gov/history/famous-cases/hurricane-katrina-fraud>
    6. INTERPOL reports showing alarming rate of increased rate of cyberattacks during COVID-19 2020 Aug 4 URL: <https://www.interpol.int/en/News-and-Events/News/2020/INTERPOL-report-shows-alarming-rate-of-cyberattacks-during-COVID-19>
    7. Johns, E. (2020). Cyber security breaches survey 2020. London: Department for Digital, Culture, Media & Sport
    8. Kumar, S., & Agarwal, D. (2018). Hacking attacks, methods, techniques and their protection measures. International Journal of Advance Research in Computer Science and Management, 4(4), 2253-2257.
    9. 64 % of Americans don’t know what to do after a data breach-Do You? , Rob Sobers,2020 Mar 29 url: <https://www.varonis.com/blog/data-breach-literacy-survey>
    10. Check Point. (2021). Cyber Security Report: 2021.
    11. Muthuppalaniappan, M., & Stevenson, K. (2021). Healthcare cyber-attacks and the COVID-19 pandemic: an urgent threat to global health. International Journal for Quality in Health Care, 33(1), mzaa117.
    12. Aldasoro, I., Frost, J., Gambacorta, L., & Whyte, D. (2021). Covid-19 and cyber risk in the financial sector (No. 37). Bank for International Settlements.
    13. Indian education sector biggest target of cyber threats, remote learning among key triggers:Report. (2022, May 1). Timesofindia.Com. Retrieved June 15, 2022, from <https://timesofindia.indiatimes.com/india/indian-education-sector-biggest-target-of-cyber-threats-remote-learning-among-key-triggers-report/articleshow/91234420.cms?utm_source=contentofinterest&utm_medium=text&utm_campaign=cppst>
    14. NATO Cooperative Cyber Defence Centre of Excellence. Cyber Definitions. Accessed: Jun 16, 2022. [Online]. Available: <https://ccdcoe.org/>
    15. Nespoli, P., Papamartzivanos, D., Mármol, F. G., & Kambourakis, G. (2017). Optimal countermeasures selection against cyber attacks: A comprehensive survey on reaction frameworks. IEEE Communications Surveys & Tutorials, 20(2), 1361-1396
    16. Al-Khater, W. A., Al-Maadeed, S., Ahmed, A. A., Sadiq, A. S., & Khan, M. K. (2020). Comprehensive review of cybercrime detection techniques. IEEE Access, 8, 137293-137311
    17. Preventing Cyber Attacks Using Penetration Testing. (2021, March 17). Softwareone. Retrieved June 16, 2022, from <https://www.softwareone.com/en-fi/blog/articles/2021/03/15/how-to-prevent-cyber-attacks-through-penetration-testing>
    18. Recent Cyber Attacks. (n.d.). Https://Www.Fortinet.Com/Resources/Cyberglossary/Recent-Cyber-Attacks. Retrieved June 17, 2022, from <https://www.fortinet.com/resources/cyberglossary/recent-cyber-attacks>
    19. Jaquet-Chiffelle, D. O., & Loi, M. (2020). Ethical and unethical hacking. In The ethics of cybersecurity (pp. 179-204). Springer, Cham.
    20. Ethical hacker Odia boy earns praise from Liberian Government. (2021, August 11). The New Indian-Express. Retrieved June 17, 2022, from <https://www.newindianexpress.com/good-news/2021/aug/11/ethical-hacker-odia-boy-earns-praise-from-liberian-government-2343171.html>
    21. Razaque, A., Amsaad, F., Khan, M. J., Hariri, S., Chen, S., Siting, C., & Ji, X. (2019). Survey: Cybersecurity vulnerabilities, attacks and solutions in the medical domain. IEEE Access, 7, 168774-168797.