REVIEW PAPER

IJETV Vol. 9, Issue 1, 2023 Print ISSN: 2394–6822 Online ISSN: 2395–4272

Cyber Threat on E-hospital - An Unnerving State of National Cyber Security System

Neelam Ahirwar

Department of Forensic Science, Kalinga University, Raipur, Chhattisgarh, India.

Abstract

The new age war ought not to be fought with guns and grenades but with machines and technologies. The is a huge paradigm shift in the pattern of the commission of crime. Some years ago, the word crime was synonymous with bloodshed, extortion and all sorts of physical violence. But now a crime can be committed anywhere in the world with just a click. Technology is a two-edged sword. On the one hand, where it is helping with online education, online banking, online healthcare facilities and making life convenient, on the other hand, all these are also increasing the risk of cyber-attacks, hacking, and identity theft-like issues. Digital forensics is a budding branch but highly in demand due to the increased financial fraud cases. In such a crime, the target can range from an individual to a whole organization being affected. It is indeed high time to understand the nitty-gritty of cyber-attacks and come out with ways to curb them. Cyber-attacks have far more fatal consequences than physical attacks.

Keywords: Cyber-attacks, Cybercrime, Hacking, Digital forensics.

Int J Eth Trauma Victimology (2023). DOI: 10.18099/ijetv.v9i01.05

Introduction

The world has not always dealt with cybercrime. The internet and information technology have stimulated economic development and innovation; however, they have also given criminals newer ways to commit crimes. Cybercrime is the most pervasive crime that severely impacts contemporary India.[1] Cybercrime is "illegal conduct in which a computer is either a tool, a target, or both". Any illegal behavior on or through a computer, the internet, or another piece of technology recognized under the Information Technology Act is called cybercrime.[2] As we progress to the twenty-first century, it will become clear that technological advancements have paved the way for all tech-savvy people to enjoy a variety of new and wonderful conveniences in daily routines. This includes the ability to learn, shop, entertain, and gain an understanding of business strategies and work processes.[3] Rapid computer technology developments have permanently altered how we conduct our daily lives. These developments make it possible for us to instantly communicate across tremendous distances and enable us to gather and organize vast volumes of information nearly without effort, tasks that would otherwise be cumbersome and expensive. Our heavy reliance on cyberspace, or the so-called Digital age, leads to cybercrime. The 1820s saw the earliest recorded computer crime.[4] Legislation all across the world is challenged by cybercrime's capacity to mutate into new and distinct antisocial behaviors that avoid the reach of existing penal law. Criminals can victimize the commoners with impunity by taking advantage of the loopholes in their own nation's legal code. Cybercriminals can also prey on the inhabitants of other countries by taking advantage of legal loopholes in their laws.[5]

Cybercrime has a very broad reach. It includes everything from lone criminals to an expanding international organized cybercrime. On the internet, scams are quite common. They overflow websites and email accounts to entice unwary victims into their webs of deceit. Spy bots and Trojan programmes make an effort to access private and business information to gather any information they can for criminal purposes. There are also many crimes of a more private character on the internet. Scammers and anyone engaging in risky activities with specific human victims frequent dating and chat platforms. Additionally, news feeds of victims of this internet or cybercrimes are frequently featured in media. Some victims have responded to the wrongdoings committed by online stalkers and game players out of personal desperation.[6]

Corresponding Author: Neelam Ahirwar, Department of Forensic Science, Kalinga University, Raipur, Chhattisgarh, India, e-mail: neelam.ahirwar@kalingauniversity.ac.in

How to cite this article: Ahirwar N. Cyber Threat on E-hospital - An Unnerving State of National Cyber Security System. Int J Eth Trauma Victimology. 2023;9(1):35-39.

Source of support: Nil

Conflict of interest: None

Received: 25/04/2023; **Received in revised form:** 15/06/2023;
Accepted: 20/06/2022; **Published:** 30/07/2022;

Cyber security threat

The three primary categories of cybercrimes are as follows: Cybercrimes against people include child pornography, harassing people via email, disseminating pornographic content, and violating someone's privacy. Such cybercrimes, if not effectively handled, harm the youth and society as a whole.

Cybercrimes against all kinds of property include computer vandalism (destroying strangers' property), spreading destructive software like the Melissa virus or the love bug,

and using alternative spyware to steal confidential company information. These crimes damaged computer networks and businesses, resulting in losses of millions of dollars on a global scale.

Cybercrimes against the government Terrorist acts that disrupt or compromise a website that is managed by the government or the military are considered cybercrimes against the government. Computer-based crimes include hacking, computer trespassing (unauthorized access), and computer fraud, which is the crime of obtaining property under pretenses in the Internet age. Similarly, there are several types of cybercrimes, including child pornography, cyberstalking, trafficking in access devices, stolen credit cards or social security numbers, computer forgery, and false users who purported to be legitimate users.[2]

Cybercrimes include a broad variety of criminal behaviors that can be either carried out simply by using computer resources or clubbed with communication devices in conjunction with more conventional methods to commit traditional crimes. Cybercrimes are covered by Section 66 of the Information Technology (Amendment) Act of 2008, which includes criminal penalties for committing any of the offenses listed in Section 43 of the ITAA 2008 if the offenses were committed with fraudulent or dishonest intentions. Aside from Section 66, the ITA 2000 amendment has expanded its scope to include rising cybercrimes.[4]

Types of cybercrime

An extensive range of possible criminal online actions is included in cyber security threats. It can be broadly categorized into two types of crimes:

1. Which can specifically target or harm computer networks or devices, such as malware, viruses, or denial-of-service attacks, and
2. That are made possible by computer networks or devices but have a primary target that is not a computer network or device, such as fraud, identity theft, phishing scams, information warfare, or cyberstalking.[6]

Crime targeting computer system

Hacking: Gaining access to a computer system without authorization to damage, steal, or destroy the data it contains is known as hacking, a more general phrase. People who are familiar with technology frequently carry it out by taking advantage of some of the system's flaws. This entails employing a variety of techniques to gather private data, including usernames, passwords, and Internet Protocol (IP) addresses, and then using that data to gain access to the computer system.[7] Hackers deploy several apps or programmes that can get past the defenses set in place by the target computer system and transmit back vital information, such as user identities, IP addresses, MAC addresses, and machine configuration, that the hacker can use to get inside the system itself. These programmes could take the shape of viruses, worms, trojan horses, or other malicious software that infects the targeted

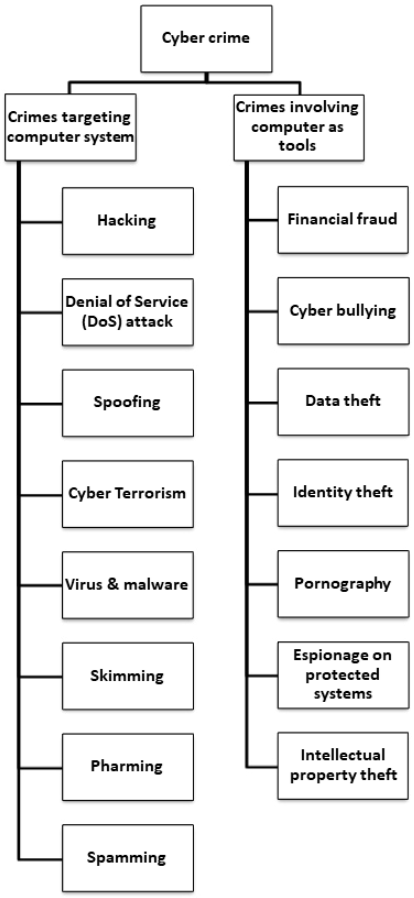

Figure 1: Types of cyber crime (Razzaq *et al.*, 2013)

system and jeopardizes its security. The hacker can take any action with the data in the computer system once they have gained access to it through hacking and have administrative powers. Other computer systems can be infected and destroyed using the computer systems.[8]

Denial of Service (DoS) attack or Distributed Denial-of-Service (DDoS) attack: In this type of attack, a Web site or server denies or disrupts a crucial service it provides, accounting for the service's intended users. A typical loss of service is the temporary loss of all network connectivity and services or the inability of a specific network service, like email, to be available. DoS attacks have occasionally been used to temporarily shut down websites. This frequently entails sending a lot of traffic, such as emails and other requests, to the server or network that is being attacked, taking up all available bandwidth before the system crashes. DDoS assaults include but are not limited to, ICMP flooding, teardrop attacks, application-level flooding, etc.[4]

Spoofing: The most popular technique used for various network attacks is spoofing. The attacker uses spoofing to disguise data packets, IP addresses, MAC addresses, and email addresses to give the impression that they are coming from different addresses.[9]

Cyber Terrorism: Terrorists these days indulge in traditional or cyber terrorism, communicate through encrypted messaging,

publish messages and recruit personnel, raise money, and produce propaganda utilizing cutting-edge technology like satellite phones. When it comes to cyber terrorism, they attack other crucial infrastructure facilities that are controlled by computer systems and disrupt computer networks and websites on a big scale. In each of these situations, the computer systems and computer resources may contain digital evidence in the form of emails, Web addresses, encrypted messages, pictures, videos, etc.[2]

Virus & malware: The majority of Internet users are impacted by the biggest crime taking place today: the spread of viruses and malware. These might be universal or tailored to a particular computer system. Viruses, worms, trojans, spyware, adware, and rootkits can all be used to inject and disseminate malicious code. These can be used to access and communicate sensitive information about the victim's computer system after being covertly installed there.[4]

Skimming: Skimming is a type of credit/debit/ATM/chip/SIM card fraud in which the information on the card is obtained using a portable device called a skimmer. Later, the information might be moved to a computer system. The creation of false credit cards is possible using information such as name, credit card number, expiration date, etc.

Pharming: Pharming is a type of attack where the user is tricked into entering sensitive information into a phoney website that impersonates a real website, such as PINs, credit card numbers, passwords, etc. In contrast to phishing, the attacker need not rely on any URLs or links in this case. Instead, it diverts visitors from a trustworthy website to a fraudulent one.

Spamming: Spamming is sending unwanted or unsolicited emails or messages to others intending to annoy or inconvenience them.[2]

Crimes involving the use of computers as tools or instruments

Financial fraud: Business fraud, investment fraud, mass marketing fraud, giving jobs abroad, Nigerian fraud, business opportunity fraud, etc. are all examples of financial frauds in which unwary people are tricked out of their money and other valuables by the promise of such chances.[5]

Cyberbullying: It is described as the act of intimidating, threatening, or harassing someone through information and communication technologies. Threats, provocative remarks, racial or ethnic slurs, LGBT shaming, attempting to infect the victim's computer with a virus, and overstuffing an email inbox are just a few examples of cyberbullying.[4]

Data theft: Data theft is the act of copying data without the owner of the computer, computer system, or computer network's consent. In the office or business, it may take the form of hacking into the system and copying confidential and sensitive information. The kind of data can be anything, including official or corporate correspondence, customer or client contact information, advertisements, user names, passwords, credit card numbers, and other pertinent papers.

Identity theft: It involves the theft of personal data used to commit fraud, including date of birth, name, PAN, passport, credit card, and email account numbers. The user may collect sensitive information through a variety of techniques, including phishing, sending links to the victim's email account and asking them to provide private information, social engineering, key-logging, etc.

Pornography: Pornography is the uploading, publication, and transmission of obscene emails, websites, chat sessions, and other online communications in any format. One of the biggest businesses on the internet is child pornography.[4]

Espionage on protected systems: This type of eavesdropping and espionage on government systems is frequently carried out by intelligence agents from rivals or close neighbours. Accessing confidential and sensitive documents is required.

Intellectual property theft: It is the theft of capital and assets based on information, trade designs, logos, ideas, and innovations, as well as content covered by copyrights owned by a person or organisation. Movies, music, and video are also included. Software and its source code have been the subject of the greatest number of intellectual property theft cases.[2]

Ransomware Attack

Ransomware has become one of the most significant cybercrimes affecting businesses over the past three years. With the help of malicious software known as ransomware, a hacker can impose some kind of access restriction on a person or organization's critical information and then demand money to remove the restriction. The most popular type of limitation used today is encryption, which essentially allows an attacker to take control of a system or hold captive user data.[10] Criminals create ransomware, a type of harmful software that prevents users from accessing their computers unless they pay a fee. As more people started working remotely during the pandemic, ransomware assaults soared. It is becoming more and more complex. In addition to encryption, other technologies are now being incorporated into ransomware's arsenal. Particularly the financial industry is frequently the target of ransomware attacks. While several nations struggle to address COVID-19, ransomware has also increased in scope and intensity, harming businesses, organizations, healthcare providers, and government agencies. Security personnel must be cautious and knowledgeable of the tactics, techniques, and processes that hackers use because ransomware continues to be one of the most serious global cyber threats to healthcare.[11] A wide variety of malicious software applications, including TorrentLocker, Locky, SamSam, CryptoLocker, CryptoWall, TeslaCrypt, KeyRanger and others, are collectively called "ransomware."[12] Typically, ransomware attacks use a Trojan, also known as a Trojan Horse, which tricks the victim into downloading or opening a malicious file when it shows up, usually as an email attachment. However, in contrast to the Trojan, the WannaCry software (used in the 2017 Ransomware attack) traveled between computers/networks automatically without human intervention. [13]

AIIMS Cyberattack

On November 23, 2022, one of India's leading premier health public institutes cripples as its internal system led the hospital to shut down. The disruptions impact hundreds of patients and professionals who use primary healthcare services, such as patient admission, discharge, and payment systems. Because the attackers changed the extensions of the infected files, the intrusion resembles a ransomware attack.[14] Several standard AIIMS processes, including OPD (Outpatient Department) registrations and blood sample reports, were unavailable as a result of the aforementioned occurrence, both inside and outside the institute. This incident affected the 'e-Hospital' application system of the National Informatics Centre (NIC), which was used at the AIIMS. The facility's inpatient and outpatient operations were overseen by the server stated earlier. This cyber-incident forced the hospital to switch from computerized to manual operations. The NIC team restored the e-Hospital application and database servers five days following the incident. Fortunately, the data backup, which was not connected to the network and thus unaffected by the event, has now been restored.[15]

Malware toolkits that find security holes and grant access to everything from email servers to entire network systems, including websites hosted on public servers, are readily available on the Dark Web for use by cybercriminals. Despite several laws and steps taken to combat it, cyberattacks against hospitals and healthcare providers are common and cause serious concern. The healthcare industry is a lucrative target for cybercriminals. Hospitals and pharmacies are only two examples of entities in the health industry that manage a lot of sensitive personal data. Terrorist organizations and cybercriminals may find such material to be of great use. Organized crime groups (OCGs) and terrorist organizations can use the stolen data to fund additional illegal activities by selling it for a high price on the Dark Web. 2020 saw a 42% increase in cyber incidents against the healthcare industry during the COVID-19 pandemic, also known as the Wuhan virus.[15]

Past cyber-attacks on the healthcare system

An infamous and catastrophic Ransomware event occurred on May 12, 2017, when the 'WannaCry' crypto-worm rendered the United Kingdom's National Health Services (NHS) inoperable for many days. Europol said the unprecedented cyber incident seriously infected 200,000 systems across 150 nations. In the wake of the "WannaCry" incident, hospitals, transportation systems, and businesses all over the world were paralyzed.[10]

The "RansomHouse" ransomware hit Colombia's Keralty global healthcare organization on November 27, 2022. The incident resulted in a disruption of the organization's website and business operations. Colombia's Keralty Healthcare runs a global network of roughly 12 hospitals and 371 medical institutions, including those in the US, Spain, Asia, and South America. Similar to a physical occurrence, a cyber incident at a hospital or healthcare facility can easily instil fear and worry in patients, guests, and employees.[16]

In June 2018, ransomware attacked Mumbai's Mahatma Gandhi Memorial (MGM) Hospital. Computer systems that were "closed" and encrypted were found by hospital administrators, along with a note from the offenders requesting a ransom in Bitcoins to regain access to the systems. According to reports, MGM Hospital lost data from 15 days' worth of billing and patient clinical information; nonetheless, the facility suffered no monetary losses.[15]

APT10, also known as StonePanda, a Chinese-backed hacking group, targeted the systems of Serum Institute of India (SII) and Bharat Biotech, two Indian vaccine manufacturers, during the Wuhan virus pandemic, according to a report published in March 2021 by the cyber-intelligence firm Cyfirma. These two companies' vaccines were a major factor in the success of Bharat's immunization campaign. By stealing intellectual property, the APT10 gang hoped to give China an edge over Indian pharmaceutical companies.[17]

Security Measures

According to officials, the AIIMS hospital served 80,000 inpatient cases and almost 15 million outpatient cases annually. The sensitive data contains the patient's personal information, such as names, ages, genders, addresses, phone numbers, and medical histories. At risk is the personal and medical information of millions of patients. If the digital health records of VVIPs, politicians, and other important figures had been hacked during the AIIMS ransomware attack, it would have been a major issue.

With the establishment of CERT-In, the National Critical Information Infrastructure Protection Center (NCIIPC), and the Indian Cyber Crime Coordination Center (IC4) Bharat's cyber security system has grown stronger over time. To maintain the overall security of our digital Bharat, the effects of such incidents must be thoroughly assessed, and the cyber ecosystem must be strengthened. The protection of cyberspace, deterring cyber enemies, and developing products for domestic and foreign usage all need to be part of the cyber security strategy. Cyber (liability) Insurance, also known as cyber risk insurance or cyber security insurance, can be employed in the case of a cyber-attack as one of the steps put in place to assure the coverage of data loss. Businesses can purchase cyber insurance as a way to help safeguard them from data breaches and other cyber security issues like malware, ransomware, and distributed denial-of-service (DDoS) attacks. Some cyber insurance policies also cover physical damage to technology, a loss of business revenue, and safeguarding virtual assets. Cyber risk insurers assess the effectiveness of an organization's cyber security framework before issuing any such policies. Strong cybersecurity frameworks provide for better coverage. Due to fragmented organizational security techniques, it may be difficult for insurers to fully comprehend the cyber security situation of an organization. As a result, organizations may obtain insurance that is not adequately targeted.[18]

Conclusion

The most crucial factors that must be taken into account while creating the architecture of a safe, dependable healthcare network are discussed in this paper. It does not offer a solution to the issue but highlights the factors that must be considered when the healthcare system is planned. One might think of the healthcare network as a cyber-physical system. A system that utilizes connected physical systems and internet technology to communicate and work. Considering the intricacy of the healthcare system is rising, new vulnerabilities in terms of security are also increasing. Since they facilitate identity theft and cybercrimes, healthcare databases are a highly sought-after target for attackers. Any denial-of-service attacks impact patients' lives on healthcare databases. Pace is the most important factor to take into account when securing healthcare databases. Healthcare transactions shouldn't be negatively impacted by an attack for a very long period, and patient history should be restored as quickly as possible. As a result, database evaluation for the healthcare system recovery should be efficient to avoid lengthy stops while implementing these actions. Attacks by ransomware on businesses are only getting started. Additionally, regardless of size, every organization is susceptible to a ransomware attack. A successful attack has considerably more consequences than just the price of the ransom. These attacks will undoubtedly increase in frequency, harm, and cost since they are profitable for those carrying them out.

References

1. Cullell, L. M. Digital Forensics and Blockchain. In *Medium, Hackernoon 2018*. https://medium.com/hackernoon/digital-forensics-and-blockchain-bf3af5e7153c?
2. *3 jhpolice_cyber_crime_investigation_manual*. (n.d.).
3. Jang-Jaccard, J., & Nepal, S. A survey of emerging threats in cybersecurity. *Journal of Computer and System Sciences 2014*, *80*(5), 973–993. https://doi.org/10.1016/j.jcss.2014.02.005
4. Ahmad Khan, S. Cyber Crime in India: An Empirical Study. *International Journal of Scientific & Engineering Research 2020*, *11*(5), 690–694. http://www.ijser.org
5. Cullell, L. M. Digital Forensics and Blockchain. In *Medium, Hackernoon 2018*. https://medium.com/hackernoon/digital-forensics-and-blockchain-bf3af5e7153c?
6. Razzaq, A., Hur, A., Ahmad, H. F., & Masood, M. Cyber security: Threats, reasons, challenges, methodologies and state of the art solutions for industrial applications. *Proceedings - 2013 11th International Symposium on Autonomous Decentralized Systems, ISADS 2013*. https://doi.org/10.1109/ISADS.2013.6513420
7. Parikh, T. P. Cyber security: Study on Attack, Threat, Vulnerability. *International Journal of Research in Modern Engineering and Emerging Technology 2017*, *5*(6), 1–7. www.raijmr.com
8. Karamchand Gandhi, V. An overview study on cyber crimes on the internet. *Journal of Information Engineering and Applications 2012*, *2*(1), 1–6. https://core.ac.uk/download/pdf/234676934.pdf
9. Dogaru, D. I., & Dumitrache, I. Cyber security in healthcare networks. *2017 E-Health and Bioengineering Conference, EHB 2017*, 414–417. https://doi.org/10.1109/EHB.2017.7995449
10. Ganesan, A., Parameshwarappa, P., Peshave, A., Chen, Z., & Oates, T. *Extending Signature-based Intrusion Detection Systems With Bayesian Abductive Reasoning 2019*. *8*(5), 2016–2018. http://arxiv.org/abs/1903.12101
11. Alawida, M., Esther, A., Isaac, O., & Al-Rajab, M. *Since January 2020 Elsevier has created a COVID-19 resource centre with free information in English and Mandarin on the novel coronavirus COVID-19 2020. The COVID-19 resource centre is hosted on Elsevier Connect, the company s public news and information*. *January*.
12. Brewer, R. Ransomware attacks: detection, prevention and cure. *Network Security*, *2016*(9), 5–9. https://doi.org/10.1016/S1353-4858(16)30086-1
13. Islam, S., Papastergiou, S., Kalogeraki, E. M., & Kioskli, K. Cyberattack Path Generation and Prioritisation for Securing Healthcare Systems. *Applied Sciences (Switzerland) 2022*, *12*(9). https://doi.org/10.3390/app12094443
14. *Delhi: Ransomware Cyber attack on AIIMS server | Delhi News - Times of India*. (n.d.). Retrieved February 20, 2023, from https://timesofindia.indiatimes.com/city/delhi/delhi-ransomware-cyber-attack-on-aiims-server/articleshow/95722736.cms
15. *AIIMS Cyber-Incident— An 'e-epidemic' Situation for Digital Bharat | Vivekananda International Foundation*. (n.d.). Retrieved February 20, 2023, from https://www.vifindia.org/article/2022/december/12/aiims-cyber-incident-an-e-epidemic-situation-for-digital-bharat#_edn14
16. Chua, J. A. Cybersecurity in the Healthcare Industry. *American Association for Physician Leadership® 2021*, *8*(1), 229–231.
17. *Chinese Hackers Targeted Serum Institute, Bharat Biotech: Cyber Firm Report*. (n.d.). Retrieved February 20, 2023, from https://www.outlookindia.com/website/story/india-news-chinese-hackers-targeted-serum-institute-bharat-biotech-cyber-firm-report/375867
18. Ministry of Health & Family Welfare. Digital Information Security in Healthcare, Act: Draft for Public Consultation. *Government of India 2017*, *211*.