INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed JournalMulti Disciplinary
Peer Reviewed Edition :

www.ijlra.com

 ISSN: 2582-6433

DISCLAIMER

ISSN: 2582-6433

EDITORIAL TEAM

EDITORS

Megha Middha

Megha Middha, Assistant Professor of Law in Mody University of Science and Technology, Lakshmangarh, Sikar

Megha Middha, is working as an Assistant Professor of Law in Mody University of Science and Technology, Lakshmangarh, Sikar (Rajasthan). She has an experience in the teaching of almost 3 years. She has completed her graduation in BBA LL.B (H) from Amity University, Rajasthan (Gold Medalist) and did her post-graduation (LL.M in Business Laws) from NLSIU, Bengaluru. Currently, she is enrolled in a Ph.D. course in the Department of Law at Mohanlal Sukhadia University, Udaipur (Rajasthan). She wishes to excel in academics and research and contribute as much as she can to society. Through her interactions with the students, she tries to inculcate a sense of deep thinking power in her students and enlighten and guide them to the fact how they can bring a change to the society

Dr. Samrat Datta

Dr. Samrat Datta Seedling School of Law and Governance, Jaipur National University, Jaipur. Dr. Samrat Datta is currently associated with Seedling School of Law and Governance, Jaipur National University, Jaipur. Dr. Datta has completed his graduation i.e., B.A.LL.B. from Law College Dehradun, Hemvati Nandan Bahuguna Garhwal University, Srinagar, Uttarakhand. He is an alumnus of KIIT University, Bhubaneswar where he pursued his post-graduation (LL.M.) in Criminal Law and subsequently completed his Ph.D. in Police Law and Information Technology from the Pacific Academy of Higher Education and Research University, Udaipur in 2020. His area of interest and research is Criminal and Police Law. Dr. Datta has a teaching experience of 7 years in various law schools across North India and has held administrative positions like Academic Coordinator, Centre Superintendent for Examinations, Deputy Controller of Examinations, Member of the Proctorial Board

ISSN: 2582-6433

Dr. Namita Jain

Head & Associate Professor

School of Law, JECRC University, Jaipur Ph.D. (Commercial Law) LL.M., UGC -NET Post Graduation Diploma in Taxation law and Practice, Bachelor of Commerce.

Teaching Experience: 12 years, AWARDS AND RECOGNITION of Dr. Namita Jain are - ICF Global Excellence Award 2020 in the category of educationalist by I Can Foundation, India.India Women Empowerment Award in the category of "Emerging Excellence in Academics by Prime Time & Utkrisht Bharat Foundation, New Delhi.(2020). Conferred in FL Book of Top 21 Record Holders in the category of education by Fashion Lifestyle Magazine, New Delhi. (2020).Certificate of Appreciation for organizing and managing the Professional Development Training Program on IPR in Collaboration with Trade Innovations Services, Jaipur on March 14th, 2019

Mrs.S.Kalpana

Assistant professor of Law

Mrs.S.Kalpana, presently Assistant professor of Law, VelTech Rangarajan Dr. Sagunthala R & D Institute of Science and Technology, Avadi.Formerly Assistant professor of Law,Vels University in the year 2019 to 2020, Worked as Guest Faculty, Chennai Dr.Ambedkar Law College, Pudupakkam. Published one book. Published 8Articles in various reputed Law Journals. Conducted 1Moot court competition and participated in nearly 80 National and International seminars and webinars conducted on various subjects of Law. Did ML in Criminal Law and Criminal Justice Administration.10 paper presentations in various National and International seminars. Attended more than 10 FDP programs. Ph.D. in Law pursuing.

Avinash Kumar

Avinash Kumar has completed his Ph.D. in International Investment Law from the Dept. of Law & Governance, Central University of South Bihar. His research work is on "International Investment Agreement and State's right to regulate Foreign Investment." He qualified UGC-NET and has been selected for the prestigious ICSSR Doctoral Fellowship.He is an alumnus of the Faculty of Law, University of Delhi. Formerly he has been elected as Students Union President of Law Centre-1, University of Delhi.Moreover, he completed his LL.M. from the University of Delhi (2014-16), dissertation on "Cross-border Merger & Acquisition"; LL.B. from the University of Delhi (2011-14), and B.A. (Hons.) from Maharaja Agrasen College, University of Delhi. He has also obtained P.G. Diploma in IPR from the Indian Society of International Law, New Delhi.He has qualified UGC – NET examination and has been awarded ICSSR – Doctoral Fellowship. He has published six-plus articles and presented 9 plus papers in national and international seminars/conferences. He participated in several workshops on research methodology and teaching and learning.

ISSN: 2582-6433

ABOUT US

INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANLAYSIS ISSN

2582-6433 is an Online Journal is Monthly, Peer Review, Academic Journal, Published online, that seeks to provide an interactive platform for the publication of Short Articles, Long Articles, Book Review, Case Comments, Research Papers, Essay in the field of Law & Multidisciplinary issue. Our aim is to upgrade the level of interaction and discourse about contemporary issues of law. We are eager to become a highly cited academic publication, through quality contributions from students, academics, professionals from the industry, the bar and the bench. INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANALYSIS ISSN 2582-6433 welcomes contributions from all legal branches, as long as the work is original, unpublished and is in consonance with the submission guidelines.

ISSN: 2582-6433

CYBERCRIME AND CYBERSECURITY AS CHALLENGES

AUTHORED BY: SHALINI PRIYA
BBA LLB 3rd year
New Law College, Pune
BHARATI VIDYAPEETH
(DEEMED to be) UNIVERSITY, PUNE
NEW LAW COLLEGE, PUNE

1. Abstract:

In today's time world is being more interconnected, and networks are being used to conduct vital transactions, therefore security is a broad topic that is becoming more significant. Cybersecurity plays an important role in the field of information technology as one of the largest problems is keeping information secure. In the digital age, cybercrime has become a global risk that is constantly changing, causing serious difficulties for people, companies, and governments. A major part of cybercrime is linked to cybersecurity, which is a tool used by cybercriminals to carry out a variety of illicit acts. This paper focuses on nature of cybercrime its challenges and difficulties that modern technology faces and the development in cyber security and crime committed in cybersecurity

Keywords: cyber security, cybercrime, social media, android apps

2. INTRODUCTION

Cyber security is protection of computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks. It's referred to as electronic information security or information technology security. It is used in a number of applications, from business to mobile computing. Now a days people send and receive data by various modes just by clicking a button and transfer their information as there is rise in technology. But whether this information is sent without any leakage? Cybersecurity is the answer to it as it protects the systems and networks from cyberattacks. With the rise of technology and the increasing dependence on internet there is

ISSN: 2582-6433

increase in cybercrime and has become a major challenge in today's digital world as we are unable to safeguard our private information. Cyber criminals are always coming up with new ways to get past security measure and steal important data. As nowadays more than 60 percent of total transaction are done online and cyber criminals use different methods range from ransomware attacks and data breaches to commit crime. So, cybersecurity has become a latest issue.

Essential elements of a successful cybersecurity plan include several levels of protection spread across computers, networks, applications, or data that one wishes to keep safe. Technology, processes, and personnel must all work together for a company to successfully fight against cyberattacks. Automating interconnections across several Cisco Security products using a single threat management system may speed up critical security operations tasks including detection, investigation, and remediation.

3. CYBER CRIME

Cybercrime is any criminal activity that is committed using digital devices or the internet it includes hacking, identity theft, cyberstalking and phishing etc it's an illegal activity in which crime is committed by using computers to steel person's identity. cybercrime increases with the increase in technology. Cybercriminals frequently take advantage of holes in computer systems or apply social engineering techniques to obtain private information without authorization or to manipulate people or organizations for financial gain or other nefarious ends.The jurisdictional problem is one of the biggest obstacles to cybercrime prosecution. Since cybercriminals can operate from any location in the world, it is challenging for law enforcement to identify which national laws apply to a given crime. This is especially important when the victim and the offender live in separate nations, as this can complicate the judicial system and cause delays in the investigation and prosecution of the case.

4. NATURE OF CYBER CRIME

Cybercrime is something which can be operated from anywhere it included a wide range of activities but they are generally divided into two categories

1. Crime which includes different threats like virus, bugs etc
2. This crime includes stalking, financial fraud or identity theft.
   These crimes are address by different countries by different ways of investigation. it is a slow process as it takes time to collect evidences and evaluation

ISSN: 2582-6433

5. CHALLENGES UNDER CYBER CRIME

- Less number of cases is registered

  In every country there is problem of cyber crime and the rate of this crime is increasing day by day but as per the crimes the cases are not registered as most of the people don't know what happens with them

- The challenge of digital evidence

  The nature of digital evidence presents another legal obstacle in the prosecution of cybercrime. It can be challenging to establish guilt beyond a reasonable doubt when using digital evidence since it is so quickly changed, removed, or concealed. Furthermore, it can be difficult and time-consuming to analyse the vast amount of digital evidence that is frequently used in cybercrime investigations.

- No harsh punishment

  Cybercrime does not always carry a severe penalty. However, there are situations where there is severe punishment. For example, when someone conducts cyberterrorism, they face severe penalty. However, in other situations, there isn't a severe penalty, which encourages the individual doing the cybercrime.

- Mostly committed by well educated people

  Because the perpetrator of cybercrime is highly technical, so the person who commit knows how to carry out the crime without being discovered by law enforcement.

- The challenge of jurisdiction

  Another legal difficulty in cybercrime prosecutions is jurisdiction. The ability of a court or other legal body to hear a case and render a decision is referred to as jurisdiction. Because cybercriminals can operate from anywhere in the world and their victims may be spread across numerous jurisdictions, jurisdiction can become complicated when it comes to cybercrime.

ISSN: 2582-6433

6. CLASSIFICATION OF CYBER CRIME

- INTERNET FRAUD

  Internet fraud is a subset of fraud or deception that uses the Internet to trick victims into parting with money or property. It may involve information concealment or misinformation being provided. Internet fraud refers to a variety of unlawful and illicit acts carried out in cyberspace rather than being regarded as a single, distinct crime. However it if different from theft its an identity theft

- CYBER WARFARE

  Cyberwarfare is the use of computers, online control systems, and networks in a combat zone or warfare setting. It covers espionage, sabotage, and cyberattack threats, and it involves both offensive and defensive activities. In cyberwarfare, a nation-state usually launches cyberattacks against another; however, terrorist groups or non-state actors may also launch cyberattacks in an attempt to advance the objectives of an adversarial state. Although there have been numerous reported cases of cyberwarfare in the past few years, there isn't a formal, accepted definition of what qualifies as a cyberattack as an act of war.

- CYBER TERRORISM

  Cyber terrorism is the use of computers and the internet to commit violent crimes that claim lives. This could involve a variety of actions using hardware or software to endanger the lives of citizens. Cyber terrorism is generally understood to be any act of terrorism carried out via the use of computers or cyberspace. It is carried by using computer servers and other devices and targets banking sectors, power plants military, essential information’s

- CYBER EXTORTION

  Cyber extortion is the act of malevolent hackers repeatedly threatening to cause denial of service attacks or other attacks against a website, email server, or computer system. In exchange for promises to halt the attacks and provide protection, these hackers demand enormous sums of money. There most common variants are ransomware and distributed denial of service attacks.

- CYBER STALKING

  This type of cyberbullying involves bombarding the victim with emails and internet

ISSN: 2582-6433

messages. In this instance, the stalkers are familiar with their targets, therefore they utilize the Internet to stalk rather than going door-to-door. To make the victims' life even more unpleasant, they start offline stalking in addition to cyberstalking if they see that the former is not having the desired result.

7. CASE LAWS AND EVENTS

In the widely reported case of **United States v. Aaron Swartz**[1], a well-known computer programmer and Internet activist from the United States was charged with breaking into the computer network of Massachusetts Institute of Technology (MIT) and downloading millions of scholarly journal articles. After being detained in 2011, Swartz was charged with wire fraud, computer fraud, and other connected offenses.

The case concerned Swartz's purported theft of millions of scholarly articles from the online repository JSTOR, which he thought ought to be publicly available. After downloading the publications using his MIT network access, Swartz was arrested and a federal investigation was launched.The prosecution claimed that by downloading a significant number of articles quickly, Swartz had broken the terms of service of JSTOR and that his acts amounted to theft of property. Supporters of Swartz countered that he was being unfairly prosecuted for his activism and belief in free and open access to knowledge, and that the accusations were overly harsh.

Numerous initiatives to improve information access and amend US computer crime laws have been launched in the years following Swartz's passing. The case serves as a sad reminder of the difficulties in prosecuting cybercrime as well as the necessity for more equitable and open legal frameworks to effectively handle the intricate problems relating to digital technology and intellectual property.

Indian saw 129 cybercrimes per lakh population in 2023[2]

Cybercrime rates in India has increased as it was reported in cybercrime complaints in NCRP per lakh population in 2023 was 129. Delhi was having the highest rate of 755 followed by Haryana and Telangana it was on mostly on customer case refund , expiry of KYC frauds which constitute of 35% of all frauds 24% was for online booking 22% AePS fraud and 11% on biometric cloning 8% on android malware.

ISSN: 2582-6433

Rising cyber crime prompts surge in cybersecurity careers [3]

There is rise of cybercrime in today's time as due to increase in technology and interconnectedness from data breaches to ransomware attacks, threat to individual business and government alike. In recent years there is rise in high profile cyber-attacks highlighting the vulnerability of digital infrastructure

8. CYBER SECURITY

cybersecurity involves protection of sensitive personal and business information through prevention, detection and response to different online attacks. there are various advantages of cybersecurity as it defends from critical attacks, helps to browse the site, website and process all the incoming and outgoing data on computer and defend from hacks and virus

The two most important security precautions that each firm takes are data security and privacy. Cybersecurity is becoming important as everything is connected with each other. We currently live in a world where all information is kept up to date digitally or online. Users of social networking sites can engage with friends and family in a secure environment. Cybercriminals would still target social networking sites in the case of home users in order to steal personal information. In addition to social networking, one must take all necessary security precautions when transacting bank business. The majority of businesses are preparing for when, not if, cyberattacks occur. Only one-third of businesses are completely confident in the security of their information, and even less confident about the security measures of their business partners. 98% of businesses are maintaining or increasing their cyber security resources, and of those, half are increasing resources devoted to online attacks this year.

Not merely an IT issue, cybersecurity poses a risk to businesses. Nevertheless, a lot of firms still haven't altered their accountability-focused culture. According to the Gartner View from the Board of Directors Survey 2022, 85% of firms still assign primary responsibility for cybersecurity to their CIO or CISO. There are different attacks on android operating system based on massive scale.

9. CHALLENGES OF CYBER SECURITY

- CLOUD ATTACKS

  Cloud computing is a service which provides there customers a wide array of cloud

ISSN: 2582-6433

platform to maximise efficiency and reduce costs.it was introduced as backup storage solution which has changed how businesses manage store and distribute data. A cloud cyberattack consists of malevolent actions directed towards an off-site service platform that uses its cloud infrastructure to offer hosting, computing, or storage services. They uses different methods as by exploiting vulnerabilities in the service software they find the weaknesses and gain access to confidential information it can se attack on server some of the largest cloud attacks in recent years are Facebook[(4)] – it was breached before august 2019 but they didn't notified there users that there personal data were stolen after that Facebook revealed details of the hack on its blog, the company reputation suffered they claimed to resolve the problem. in order to resolve a privacy suit with federal trade commission which involved a fine of $5 billion.

LinkedIn – in 2021, it Another site compromised by data scraping was LinkedIn. The material largely affected 700 million LinkedIn profiles and was available to the public. However, in June 2021, the hack's data was published on a dark web forum. LinkedIn clarified that no private or sensitive information was revealed. Additionally, the business claimed that the occurrence just broke the terms of service.

- WEB SERVERS

  Attacks to transmit dangerous code or retrieve data from web applications are still a possibility. Cybercriminals utilize hacked legitimate web servers to spread their harmful code. However, attacks aimed at stealing data are also a serious concern, as they frequently attract media attention. Our focus now has to be more on safeguarding web servers and web applications. In particular, web servers provide these cybercriminals with the ideal platform for data theft. Therefore, it is imperative to always utilize a safer browser, particularly while making crucial transactions, to avoid being a victim of these crimes.

- RANSOMWARE ATTACKS

  Malicious malware known as ransomware has the ability to permanently harm your computer and its contents. By locking the device or encrypting the files on it, it prevents you from accessing your data. Ransomware attackers typically demand money in exchange for unlocking your computer or restoring access to your data. This is frequently

ISSN: 2582-6433

accomplished through websites that demand cryptocurrency payments or anonymous emails.

- PHISHING ATTACKS

  Phishing is a type of social engineering that is often used to steal credit card numbers, usernames, and other personal information. In this cyber security issue, a malevolent actor poses as a trustworthy party and sends emails, texts, or messages to the target that is at risk.

- MOBILE NETWORKS

  We can communicate with anyone, anywhere in the globe, these days. But security is a major worry for these mobile networks. Nowadays, as more people use devices like tablets, phones, PCs, and other gadgets, firewalls and other security measures are becoming more porous. These devices also call for additional security measures on top of those offered by the programs they use. We need to be aware of these mobile networks' security concerns at all times. Furthermore, mobile networks are particularly vulnerable to these cybercrimes, thus caution must be exercised when it comes to any security concerns.

10. ROLE OF SOCIAL MEDIA IN CYBER SECURITY

In today's time world has become a global platform where there is constant interaction with each other through various modes and sides and commonly used platform are social media like Facebook, Instagram, Twitter and more and they have became a part of everyday life it contains a vast amount of information and authentic it does have security but still they cannot escape cyber attacks

In an increasingly linked world, where social interactions are common, businesses need to come up with innovative strategies for safeguarding personal data. Social media will significantly increase personal cyber dangers and plays a major role in cyber security. The use of social media among employees is rapidly increasing, and with it, the risk of an attack. Since the majority of people use social media or social networking sites virtually daily, it has grown to be a major platform for cybercriminals to hack personal data and steal valuable data as people easily get attracted by these platforms Social media not only allows everyone the ability to share economically sensitive information, but it also gives the same ability to spread incorrect

ISSN: 2582-6433

information, which may be just as harmful. One of the rising threats noted in the Global Risks 2013 repository is the quick dissemination of misleading information via social media

In a world where we're quick to give up o

11. TECHNIQUES OF CYBER SECURITY[5]

- ANTI-VIRUS SOFTWARE

  Computer programs known as antivirus software are designed to identify, stop, and eliminate harmful software, including worms and viruses. The majority of antivirus software comes with an auto-update capability that allows the application to download virus profiles as soon as they are found, allowing it to scan for new infections right away. Every system needs anti-virus software as a basic requirement.

- FIREWALLS

  A firewall is a hardware device or software application that helps block viruses, worms, and hackers from infecting your computer through the Internet. Every message that enters or exits the internet is filtered by the firewall, which checks each one and deletes any that don't fit the predetermined security requirements. Firewalls are crucial in identifying malware because of this.

- ENCRYPTION

  Encryption is the process of converting data into a code to prevent unauthorized access. It is used to protect sensitive information during storage, transmission, and processing.

- AUTHENTICATION AND ACCESS CONTROL

  Robust authentication techniques, such multi-factor authentication, along with access control mechanisms serve to guarantee that systems and data are only accessed by authorized personnel. Using the user name and password to protect the information

- SECURITY PATCHING

  Regularly applying security patches and updates to operating systems, applications, and firmware helps address vulnerabilities and protect against known exploits

ISSN: 2582-6433

- MALWARE SCANNERS

  This software typically checks all of the system's files and papers for dangerous viruses or malicious code. Examples of dangerous software that are frequently bundled together and referred to as malware include viruses, worms, and Trojan horses.

- NETWORK SEGMENTATION

  Dividing a network into segments helps contain security breaches and limit the potential damage by restricting lateral movement within the network.

- SECURITY AWARNESS TRAINING

  By teaching users about social engineering threats, security best practices, and how to spot phishing attempts, the human element in cybersecurity incidents can be considerably decreased.

12. CONCLUSION

With the usage of networks to conduct vital transactions, the world is growing increasingly interconnected, making computer security a broad topic that is becoming increasingly significant. In the digital age, cybercrime presents a serious challenge to law enforcement. Cybercrime poses jurisdictional challenges and anonymity, making it difficult to identify and prosecute offenders with every new year that goes by, cybercrime and information security continue to take different turns. Organizations face challenges in protecting their infrastructure not only from emerging and disruptive technologies but also from new cyber tools and attacks that emerge on a daily basis. Securing infrastructure effectively requires not only new platforms and intelligence, but also new approaches. Although there isn't a perfect way to stop cybercrimes, we should make every effort to reduce them so that we may continue to use the internet safely and securely

13. REFERENCES

1. Case law - United state v. Aaron Swartz case 2011 Criminal No. 11-10260-NMG (D. Mass. Aug. 1, 2011) https://casetext.com/case/united-states-v-swartz-8 (last visited 27.01.2024) 6:50pm
2. Article on cybersecurity https://timesofindia.indiatimes.com/india/rising-cyber-crime-prompts-surge-in-cybersecurity-careers/articleshow/105363450.cms
3. Times of India Article https://timesofindia.indiatimes.com/topic/Cyber-crime/news/2

ISSN: 2582-6433

4. Cybercrime article on https://www.geeksforgeeks.org/cyber-crime/ (last visited on 28.01.2024)
5. The Indian express.com https://indianexpress.com/article/india/a-timeline-of-the-pegasus-snooping-scandal/ (last visited 27.1.2024)
6. A blog on cloud security breaches by https://www.arcserve.com/blog/7-most-infamous-cloud-security-breaches (last visited 28.01.2024)
7. How cyber security works https://www.cisco.com
8. A study of cyber security https://www.researchgate.net/publication
9. Cyber Security: Understanding Cyber Crimes- Sunit Belapure Nina Godbole