INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed JournalMulti Disciplinary
Peer Reviewed Edition :

www.ijlra.com

 ISSN: 2582-6433

DISCLAIMER

No part of this publication may be reproduced or copied in any form by any means without prior written permission of Managing Editor of IJLRA. The views expressed in this publication are purely personal opinions ofthe authors and do not reflect the views of the Editorial Team of IJLRA.

Though every effort has been made to ensure that the information in Volume 2 Issue 7 is accurate and appropriately cited/referenced, neither the Editorial Boardnor IJLRA shall be held liable or responsible in any manner whatsever for any consequences for any action taken by anyone on the basis of information in the Journal.

Copyright © International Journal for Legal Research & Analysis

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

CYBER EXTORTION IN INDIA AND ITS LEGISLATIVE MEASURES

AUTHORED BY - R. USHA

INTRODUCTION

In the digital era, where technology plays a crucial role in our daily lives, cybercriminals have identified new and more insidious ways to exploit individuals and organizations. One such nefarious act is cyber extortion, a malicious method aimed at coercing victims into surrendering their valuable resources, sensitive information, or money under the threat of releasing compromising or damaging materials online. According to the report by Orange Cyberdefense, which reveals that India has witnessed a 97% increase in cyber extortion victims in 2023. With the unstoppable rise of cybercrime, it is essential to understand the concept of cyber extortion, legal challenges and the countermeasures one can adopt to safeguard against this growing threat.

CYBER EXTORTION

Cyber extortion is a type of digital crime, where individuals with malicious intent confiscate someone's confidential information and demand payment in order to prevent its exposure to the public. Cybercriminals have control over computer systems and websites, and they leverage this power to blackmail their victims until their demands are met. The person who blackmails the victim is called cyber extortionist.

Any business, organization, or person that depends on centralized digital operations, digital tools, or online customer relationship management systems can be vulnerable to cyber extortionist. Eg; - E-commerce companies, medical sectors, financial advisors, etc[1].

[1] Kimberlee Leonard, What Is Cyber Extortion?, Updated Nov 07, 2023, What Businesses Should Know About Cyber Extortion - business.com, accessed - 24 Dec 2023.

ISSN: 2582-6433

STAGES OF CYBER EXTORTION

The cyber extortion attacks typically involve the following stages:

1. Unauthorized Entry: The attacker gains unauthorized access to the victim's IT resources.
2. Expansion: The attacker expands their access by persistently gaining control, conducting reconnaissance, broadening their access, and sharing it with others.
3. Assessment: The attacker evaluates the victim's strengths and weaknesses, including data repositories, financial status, and operational infrastructure. This information helps them refine their attack strategy.
4. Preparation: The attacker modifies the environment to maximize their advantage in subsequent phases. This may involve actions such as destroying backups, dismantling security measures, or monitoring systems.
5. Exploitation: The attacker actively threatens the confidentiality, integrity, or availability of the victim's information resources. Common methods include deploying ransomware, extracting data to their own systems, launching denial-of-service attacks, or a combination of these.
6. Extortion: The attacker demands payment or services from the victim in exchange for restoring the availability, integrity, or confidentiality of the compromised data or technology resources[2].

EXTORTION MESSAGES

Extortion messages are commonly used by cybercriminals to create a sense of urgency and fear in their victims. These messages typically share similar traits with the goal of pressuring the victim into compliance.

1. One method often used is claiming that the criminals have obtained one of the victim's account passwords, tricking them into believing their confidential information has been compromised.
2. Another common type of extortion email involves the threat of releasing embarrassing photographs that the hackers claim to have obtained[3].

[2] Sherri Davido, Matt Durrin, Karen Sprenger, Ransomware and Cyber Extortion Response and Prevention, 2023, Anddison Wesley, ISBN-13: 978-0-13-745033-6, ISBN-10: 0-13-745033-8, accessed - 29 Nov 2023.
[3] By Adrian, What to do when you receive an extortion email, Internet Security, June 19, 2020, What to do when you receive an extortion email (internetsecurity.tips), accessed - 28 Nov 2023

ISSN: 2582-6433

DIFFERENT TYPES OF CYBER EXTORTION TECHNIQUES

The most common cyber extortion attacks are,

a) Denial of Service (DDoS) attacks: Cybercriminals target servers and disrupt access to data. They demand payment to stop ongoing attacks or threaten to conduct an attack if payment is not made.
b) Ransomware: Victims find their devices infected with malware, making it impossible to access data. This is usually contracted by unintentionally downloading the malware through infected email attachments, compromised websites, or clicking on pop-up ads. The only way to regain access is to pay a ransom to the hacker.

Other types,

a. Database ransom attacks: Hackers identify and hijack vulnerable databases, exploiting weaknesses in systems like MySQL, Hadoop, MongoDB, and ElasticSearch. Breached servers are often replaced with ransom notes, demanding payment in Bitcoin to restore the data.
b. Doxing: This involves intentionally revealing a victim's personal or private information, such as their address, phone number, or financial records. Hackers use this tactic to cause harm or distress and may make threats against specific individuals or groups if their demands are not met[4].
c. Sextortion: Sextortion refers to a type of cyber extortion in which an individual initially gains control over sexual videos or private images belonging to the victim and threatens to distribute explicit or sexually suggestive material of a person unless they comply with certain demands. These demands often include sending more explicit content, providing money, or engaging in sexual activities to satisfy the blackmailer[5].
d. Malvertising, short for malicious advertising, refers to the practice of using online advertisements to spread malware or engage in other malicious activities. When users click on these malicious ads, they may be redirected to websites hosting exploit kits, which attempt to exploit vulnerabilities in the user's software to install malware on their devices.

[4] Vaibhav Ruparel, CYBER EXTORTION, Published Oct 31, 2023,CYBER EXTORTION (linkedin.com), accessed - 26 Nov 2023.
[5] Gautam Chaudhary, All about cyber extortion, December 24, 2022, All about cyber extortion - iPleaders, accessed - 26 Nov 2023.

ISSN: 2582-6433

e. Corporate account takeover (CATO): It occurs when a perpetrator pretends to be the company's website or email and urges for wire or ACH transactions. The funds are then transferred to an account that appears valid but is actually under the control of the attacker. Businesses that have limited control over their online banking platforms are especially vulnerable to this form of fraudulent activity.

LAWS OF CYBER EXTORTION

The term "cyber extortion" is not defined in any legislations in India. However, individuals accused of cyber extortion can be charged with offenses under the Indian Penal Code, 1860, Information Technology Act, 2000 and other Acts.

INDIAN PENAL CODE, 1860

SALE, ETC., OF OBSCENE BOOKS, ETC: Section 292 of the Indian Penal Code (IPC), It prohibits the sale or distribution of obscene materials.in any forms or any other objects which can be relevant in cases where perpetrators demand payment or resources in exchange for not divulging explicit or private information that could harm an individual's reputation or personal life.

EXTORTION: Section 383 addresses, whoever intentionally puts any person in fear of any injury to that person, or to any other, and thereby dishonestly induce them to surrender property, valuable securities, or anything signed or sealed which may be converted into a valuable security. This section can be applicable in cases where cybercriminals threaten to harm an individual or their personal or professional reputation unless they pay a ransom or provide other forms of compensation.

CRIMINAL INTIMIDATION: Section 503 says, whoever threatens another person with harm to their person, reputation, or property with the intention of causing fear or compelling them to act against their will[6]. This provision can be relevant in cases where cyber extortionists make threats to coerce victims into providing sensitive information, accessing financial accounts, or carrying out illegal activities.

[6] Nehal Misra, What can I do if someone is blackmailing me online, June 5, 2021, What can I do if someone is blackmailing me online - iPleaders, accessed - 22 Nov 2023.

ISSN: 2582-6433

VOYEURISM: Section 354C of the IPC, whoever watches, or captures the image of a woman engaging in a private act in circumstances where she would usually have the expectation of not being observed by the perpetrator or by any other person. It is relevant in cases where cyber extortionists engage in the non-consensual capturing, recording, or dissemination of intimate images or videos of individuals without their knowledge or consent. Perpetrators may use these materials as leverage to extort money or manipulate their victims.

INFORMATION TECHNOLOGY ACT. 2000

a. DAMAGE TO COMPUTER, COMPUTER SYSTEM, ETC: Sections 43 of the IT Act, 2000, states that anyone who engages in activities such as accessing, downloading, copying, introducing viruses, damaging, disrupting, denying access, providing assistance, tampering with services, destroying information, or altering computer source code without permission of the owner or any other person who is in charge of a computer, computer system or computer network is liable to pay damages as compensation to the affected person. The Act defines various terms that are directly relevant to cyber extortion cases.

i. "Computer contaminant" refers to a set of instructions that modify, destroy, or disrupt computer systems, which cyber extortionists may use to compromise security.

ii. "Computer database" refers to information or knowledge prepared in a structured manner for computer use, often targeted by hackers seeking valuable data for extortion purposes.

iii. "Computer virus" refers to any programming or instruction that damages or affects the performance of computer resources, sometimes used as a means of coercing victims.

iv. "Damage" encompasses activities such as destruction, alteration, deletion, or modification of computer resources, including unauthorized access resulting from cyber extortion attempts.

v. "Computer source code" refers to the programming and design of computer resources that cybercriminals may target or manipulate for their illicit purposes[7].

[7] Information Technology Act, 2000.

ISSN: 2582-6433

b. COMPENSATION FOR FAILURE TO PROTECT DATA: Section 43A of the Act, in cases of cyber extortion, where a body corporate, which includes companies, firms, or any other legal entities, fails to protect sensitive personal data or information due to negligence in implementing and maintaining reasonable security practices and procedures, causing wrongful loss or gain to any person, they shall be liable to pay damages as compensation to the affected individual. This provision serves as a deterrent for organizations and incentivizes them to prioritize data security.

c. TAMPERING WITH COMPUTER SOURCE DOCUMENTS: Section 65 of the act, SECTION 65: Tampering with computer source documents, such as altering or destroying computer source code required by law to be maintained. In cyber extortion cases, perpetrators may tamper with computer source documents to hide traces of their activities or disrupt the victim's systems for coercive purposes.

d. VIOLATION OF PRIVACY: Section 66E of the Act, it involves capturing, publishing, or transmitting images of a person's private area without their consent, infringing upon their privacy, can be applicable in certain cyber extortion scenarios. Perpetrators may exploit stolen or sensitive images to extort individuals or organizations.

e. PUBLISHING AND TRANSMITTING OBSCENCE MATERIAL IN ELECTRONIC FORM: Section 67 of the Act, Publishing and transmitting obscene material in electronic form with the intent to deprave and corrupt individuals who are likely to come across such content is a punishable offense. In cyber extortion cases, perpetrators may threaten to publish explicit or compromising material unless the victim complies with their demands.

f. PUBLISHING OR TRANSMITTING OF MATERIAL CONTAINING SEXUALLY EXPLICIT ACT, ETC., IN ELECTRONIC FORM: Section 67A of the IT Act, Publishing or transmitting material containing sexually explicit acts or conduct in electronic form is prohibited under this section. In cyber extortion cases, perpetrators may use sexually explicit material as leverage to extort money or other benefits from their victims.

g. PUBLISHING OR TRANSMITTING OF MATERIAL DEPICTING CHILDREN IN SEXUALLY EXPLICIT ACT, ETC., IN ELECTRONIC FORM: Section 67B of the IT Act, 2000, This section explicitly deals with the publishing, transmitting, or promoting of material that depicts children engaged in sexually explicit acts or conduct in electronic form. Individuals who create text or digital images, collect, browse, download, advertise,

ISSN: 2582-6433

promote, exchange, or distribute material in electronic form depicting children in an obscene, indecent, or sexually explicit manner are liable.

OTHER ACTS

a. According to Section 108(1)(i)(a) of the Criminal Procedure Code, the victim has the right to contact a magistrate in their area and report any suspicion of distributing obscene material. The magistrate has the power to detain and require the suspected individual to sign a bond to prevent them from disseminating such material. This serves as a deterrent for the accused, and the victim can file a complaint without needing concrete evidence[8].
b. The Protection of Children from Sexual Offences Act, 2012, targets issues of sexual exploitation of children, while the Information Technology Act, 2000, covers sexual offenses related to cybercrime.

CASE LAWS

The UHBVN Ransomware Attack: The Uttar Haryana Bijli Vitran Nigam, a government-owned power distribution company for North Haryana, fell victim to a ransomware attack on March 17, 2021. The hackers stole billing data and demanded a ransom of Rs. 1 crore (approximately $10 million) in bitcoins to return the customer data.

The Mirai Botnet Malware Attack: This botnet malware targeted home routers and IoT devices, affecting around 2.5 million IoT devices, including a significant number in India. Capable of exploiting unpatched vulnerabilities, this self-propagating malware gained access to networks and systems[9].

AIIMS Ransomware Attack: cyber terrorists recently attacked the eHospital server of the All-India Institute of Medical Sciences (AIIMS) in Delhi. This cyber-attack has put the health data of top ministers at risk. The incident occurred on October 18, and it affected the digitized data of

[8] Nehal Misra, What can I do if someone is blackmailing me online, June 5, 2021, What can I do if someone is blackmailing me online - iPleaders, accessed - 22 Nov 2023.
[9] *Gautam Chaudhary,* All about cyber extortion, December 24, 2022, All about cyber extortion - iPleaders, accessed - 26 Nov 2023.

ISSN: 2582-6433

the hospital, including patient records and databases[10]. The IT division of AIIMS promptly took action and isolated the affected part of the server to prevent further damage. The report mentions that the attackers may have targeted the hospital's server to obtain sensitive information about the ministers and potentially use it for nefarious purposes. The AIIMS administration has lodged a complaint with the police's cyber cell, and an investigation is currently underway.

CYBER EXTORTION AND MEITY

In 2017, Ministry of Electronics and Information Technology (MeitY) reached out to various entities, including the Reserve Bank of India (RBI), the National Informatics Centre (NIC), and the bodies responsible for cybersecurity in different states. The aim was to inform and educate them about the WannaCry ransomware threat and provide necessary guidelines to protect against it[11].

Apart from being advisory, MeitY can organize awareness campaigns to educate the public about the risks and consequences of cyber extortion. It can collaborate with law enforcement agencies to coordinate efforts in investigating and prosecuting cyber extortion cases. It can establish an incident response system to quickly respond to cyber extortion attacks.

MEASURES TO PREVENT CYBER EXTORTION

1. Install a reliable antivirus and antimalware software on your devices to detect and prevent malicious software. Regularly scan your devices for any potential threats.
2. Develop and enforce strong password policies that require employees to use unique and complex passwords and change them regularly.
3. Restrict access to sensitive data and systems, only allowing authorized individuals to access and modify them.
4. Implement strong email security measures, such as email filtering, to prevent phishing attacks and malicious email attachments.
5. Limit the amount of personal information you share on social media platforms, as

[10] Economic Times, Cyber terrorists attack AIIMS-Delhi eHospital server, health data of top ministers under threat, Updated On Nov 25, 2022 at 03:49 PM IST, Cyber terrorists attack AIIMS-Delhi eHospital server, health data of top ministers under threat, ET Government (indiatimes.com), accessed - 01 Dec 2023.
[11] Times of India, MeitY reaches out to RBI, others against Wanna Cry ransomware, May 14, 2017, 22:47 IST, MeitY reaches out to RBI, others against Wanna Cry ransomware - Times of India (indiatimes.com), accessed - 01 Dec 2023.

ISSN: 2582-6433

cybercriminals can use this information to target you.

6. Stay informed about different types of cyberextortion scams, such as phishing, impersonation, or sextortion.
7. Stay vigilant and monitor your online accounts for any suspicious activity. If you become a victim of cyberextortion or encounter suspicious activities, report the incident to the appropriate authorities, such as the local law enforcement or country's cybercrime unit.

CONCLUSION

The rise of advanced technologies has opened up new avenues for cybercriminals to exploit individuals, businesses, and even entire nations. To combat this, robust firewalls, encryption methods, employee training, and legislation punishing cyber extortion perpetrators are essential. Being a victim of cyber extortion can cause severe emotional distress, including fear, anxiety, and humiliation. Individuals may become more skeptical and cautious while interacting online due to a cyber-extortion incident. It is also essential to report any incidents to the appropriate authorities and seek professional guidance to handle the situation effectively Cyber extortion attacks served as a stark reminder of the vulnerabilities faced by individuals and institutions in the digital age and emphasizes the importance of raising awareness and promoting international cooperation to collectively combat cyber extortion. By taking proactive steps, such as implementing robust cybersecurity measures, increasing awareness, and fostering international collaboration, we can create a safer digital environment for everyone.

REFERENCE

STATUES

1. Indian Penal Code, 1860.
2. Information Technology Act, 2000.
3. Code of Criminal Procedure Code, 1973.
4. Protection of children from sexual offences Act, 2012.

WEBLIOGRAPHY

1. Kimberlee Leonard, What Is Cyber Extortion?, Updated Nov 07, 2023, What Businesses Should Know About Cyber Extortion - business.com, accessed - 24 Dec 2023.
2. Sherri Davido, Matt Durrin, Karen Sprenger, Ransomware and Cyber Extortion Response and Prevention, 2023, Anddison Wesley, ISBN-13: 978-0-13-745033-6, ISBN-10: 0-13-

ISSN: 2582-6433

745033-8, accessed - 29 Nov 2023.

3. By Adrian, What to do when you receive an extortion email, Internet Security, June 19, 2020, What to do when you receive an extortion email (internetsecurity.tips), accessed - 28 Nov 2023.
4. Vaibhav Ruparel, CYBER EXTORTION, Published Oct 31, 2023, CYBER EXTORTION (linkedin.com), accessed - 26 Nov 2023.
5. Gautam Chaudhary, All about cyber extortion, December 24, 2022, All about cyber extortion - iPleaders, accessed - 26 Nov 2023.
6. Nehal Misra, What can I do if someone is blackmailing me online, June 5, 2021, What can I do if someone is blackmailing me online - iPleaders, accessed - 22 Nov 2023.
7. Economic Times, Cyber terrorists attack AIIMS-Delhi eHospital server, health data of top ministers under threat, Updated On Nov 25, 2022 at 03:49 PM IST, Cyber terrorists attack AIIMS-Delhi eHospital server, health data of top ministers under threat, ET Government (indiatimes.com), accessed - 01 Dec 2023.
8. Times of India, MeitY reaches out to RBI, others against Wanna Cry ransomware, May 14, 2017, 22:47 IST, MeitY reaches out to RBI, others against Wanna Cry ransomware - Times of India (indiatimes.com), accessed - 01 Dec 2023.