LEGAL FRAMEWORK FOR COMBATTING RANSOMWARE ATTACKS - POLICIES AND RECOMMENDATIONS

P. Priya Raghavendra, Maharashtra National Law University, Nagpur

ABSTRACT

The increasing prevalence and sophistication of ransomware attacks pose significant challenges to individuals, businesses, governments, and critical infrastructure globally. This legal research paper titled "Legal Framework for Combatting Ransomware Attacks - Policies and Recommendations" undertakes a comprehensive exploration of the existing legal framework and policies aimed at combatting ransomware attacks in India.

The paper critically analyzes the inadequacies and gaps in the current legal provisions, examines the international legal frameworks and best practices, evaluates the effectiveness of law enforcement capabilities and cybersecurity measures, and proposes actionable recommendations and strategies to enhance the legal framework, policies, and strategies for combatting ransomware attacks in India.

The research objectives encompass examining the existing legal framework, analyzing international legal frameworks, assessing law enforcement capabilities, evaluating cybersecurity measures, and formulating recommendations for improving the legal framework and mitigating the risks and impacts of ransomware attacks. The paper concludes with comprehensive recommendations and suggestions for strengthening the legal framework, policies, and strategies, fostering a safer, more resilient, and secure cyberspace in India, and mitigating the risks and impacts of ransomware attacks effectively.

INTRODUCTION

In recent years, ransomware attacks have emerged as one of the most significant and prevalent cyber threats, posing substantial risks to individuals, businesses, governments, and critical infrastructure globally. A ransomware attack is a type of malicious cyber attack that involves the deployment of malicious software to encrypt the victim's data or block access to their computer systems, followed by a demand for ransom payment, usually in cryptocurrency, in exchange for the decryption key or the restoration of access to the compromised data or systems. The perpetrators of ransomware attacks exploit vulnerabilities in computer systems, networks, and software, leveraging sophisticated techniques and tactics to infiltrate, infect, and compromise the target systems.

The impact of ransomware attacks extends beyond financial losses, encompassing operational disruptions, data breaches, reputational damage, and national security threats, highlighting the critical need for robust legal frameworks, policies, and strategies to combat and mitigate the risks and impacts of ransomware attacks effectively. The legal framework for combatting ransomware attacks encompasses various aspects, including defining the offense, establishing legal procedures and penalties, enhancing law enforcement capabilities, promoting cybersecurity measures, encouraging international cooperation and collaboration, and strengthening incident response and recovery mechanisms.

This legal research paper aims to analyze the existing legal frameworks, policies, and strategies for combatting ransomware attacks in India, evaluate their effectiveness and adequacy in addressing the evolving challenges posed by ransomware attacks, and provide recommendations and suggestions for enhancing the legal framework, improving cybersecurity measures, and mitigating the risks and impacts of ransomware attacks in India effectively.

RESEARCH OBJECTIVES

A) To identify and analyze the existing laws, regulations, and legal provisions relevant to combatting ransomware attacks in India.

B) To evaluate the adequacy, effectiveness, and gaps in the current legal framework in addressing the challenges and complexities of ransomware attacks.

C) To identify and recommend cybersecurity measures, strategies, and guidelines to strengthen

the resilience and defenses against ransomware attacks.

RESEARCH QUESTIONS

a. What are the international legal provisions and best practices for combatting ransomware attacks?

b. What are the challenges and barriers faced by law enforcement agencies in combatting ransomware attacks effectively?

c. What recommendations and suggestions can be formulated to improve the legal framework, policies, and strategies for combatting ransomware attacks in India based on the analysis?

HYPOTHESIS

a. The existing legal framework in India lacks comprehensive and specific penalties, sanctions, and legal procedures to deter, investigate, and prosecute ransomware attacks and cybercriminals effectively.

b. The international legal frameworks and best practices provide a more comprehensive, detailed, and effective approach to combatting ransomware attacks compared to the Indian context.

c. The development and implementation of enhanced legal provisions, penalties, and legal procedures can strengthen the deterrence, detection, investigation, and prosecution of ransomware attacks and cybercriminals in India.

MEANING AND DEFINITION OF 'RANSOMWARE ATTACK":

A ransomware attack is a type of malicious software (malware) attack that encrypts the victim's files or locks the victim out of their device, rendering the data inaccessible. The attacker then demands a ransom payment, usually in cryptocurrency, from the victim to decrypt the files or restore access to the device.[1]

[1] Ransomware Attack – What is it and How Does it Work? https://www.checkpoint.com/cyber-hub/threat-prevention/ransomware/

The term "ransomware attack" can be defined as:

"*A form of cyberattack involving the deployment of malicious software (ransomware) to encrypt the victim's data or restrict access to their device. The attacker then demands a ransom payment from the victim, typically in cryptocurrency, in exchange for the decryption key or to restore access to the compromised device or data.[2]

CHARACTERISTIC FEATURES OF RANSOMWARE ATTACKS:

- **Encryption of Data:**

Ransomware attacks typically involve the encryption of the victim's data, making it inaccessible to the victim. The attacker holds the decryption key and demands a ransom payment for its release.[3]

- **Ransom Payment:**

The attacker usually demands a ransom payment from the victim, often in cryptocurrency, to provide the decryption key or restore access to the compromised device or data.

- **Threat of Data Loss or Disclosure:**

In addition to encrypting the victim's data, ransomware attackers often threaten to publish or sell the victim's data if the ransom is not paid, adding a layer of extortion to the attack.

- **Time-sensitive Demands:**

Ransomware attackers often impose a deadline for the ransom payment, adding urgency and pressure on the victim to comply with the attacker's demands.

TYPES OF RANSOMWARE ATTACKS:

A. Encrypting Ransomware:

Encrypting ransomware is a type of ransomware that encrypts the victim's files or data, making

[2] What is ransomware, https://www.ibm.com/topics/ransomware
[3] Australian Signals Directorate, https://www.cyber.gov.au/threats/types-threats/ransomware

them inaccessible. The attacker holds the decryption key and demands a ransom payment for its release. This type of ransomware encrypts the victim's files or data, making them inaccessible.[4]

Example: WannaCry Ransomware, cryptocurrency, etc.

- WannaCry Ransomware Attack (2017): The WannaCry ransomware attack was a global cyberattack that affected over 200,000 computers in 150 countries, encrypting data and demanding ransom payments in Bitcoin.

B. Locker Ransomware:

Locker ransomware locks the victim out of their device, preventing access to the device's operating system. The attacker demands a ransom payment to restore access to the compromised device. Examples include Winlocker and GPCoder.[5]

- US v. Mihai Alexandru Isvanca & Eveline Cismaru (2018): Mihai Alexandru Isvanca and Eveline Cismaru were indicted for their involvement in the distribution of ransomware, including Winlocker, which targeted victims in the United States.

C. Doxware or Leakware:

Doxware or leakware not only encrypts the victim's data but also threatens to publish or disclose the victim's data if the ransom is not paid. The attacker uses the threat of data loss or disclosure to extort the victim into paying the ransom. Examples include Maze

- State of Utah v. Alexander Filinov (2020): Alexander Filinov was charged for his involvement in the distribution of Maze ransomware, which not only encrypted victims' data but also threatened to publish the data if the ransom was not paid.

D. Ransomware as a Service (RaaS)

Ransomware as a Service (RaaS) is a type of ransomware where the attacker leases or sells

[4] Ransomware Attacks and Types – How Encryption Trojans Differ, https://www.kaspersky.co.in/resource-center/threats/ransomware-attacks-and-types
[5] 5 TYPES OF RANSOMWARE Kurt Baker - January 30, 2023, https://www.crowdstrike.com/cybersecurity-101/ransomware/types-of-ransomware/

ransomware software to other cybercriminals to conduct ransomware attacks. RaaS allows cybercriminals with limited technical skills to launch ransomware attacks, increasing the proliferation and diversity of ransomware attacks.

Example: Sodinokibi (REvil) Ransomware

- US v. Yaroslav Vasinskyi (2021): Yaroslav Vasinskyi was charged for his involvement in the distribution of Sodinokibi (REvil) ransomware as part of a RaaS scheme, allowing other cybercriminals to conduct ransomware attacks using the Sodinokibi ransomware software.

INTERNATIONAL LEGAL FRAMEWORK FOR COMBATTING RANSOMWARE ATTACKS:

Ransomware attacks, where attackers encrypt a victim's data and demand a ransom for decryption, pose a significant threat in the digital age. The international community has responded by developing a patchwork of legal frameworks to deter, investigate, and prosecute these attacks. This section delves into the key aspects of this international legal landscape, analyzing relevant legal provisions and case law.

INTERNATIONAL TREATIES AND CONVENTIONS:

- **Budapest Convention on Cybercrime (2001):** This Council of Europe treaty obligates signatories to criminalize certain cybercrime offenses, including illegal access to computer systems and data interference. It also establishes a framework for international cooperation in investigations and prosecutions.

a) Article 2: Offences against computer systems and data: This article criminalizes a range of offenses, including:[6]

* Illegal access to a computer system (sec 2(a))

* Illegal interception of computer data (sec 2(b))

* Data interference (sec 2(c))

[6]Article 2: Offences against computer systems and data (Council of Europe, Convention on Cybercrime, ETS No. 185, art. 2 (2001)

* Ransomware attacks often involve these offenses when attackers gain unauthorized access to a victim's system, intercept data by encrypting it, and interfere with normal operations by rendering data inaccessible.

b) Article 16: Search and seizure of computer data: This article allows signatory countries to take necessary measures to search or seize computer data related to cybercrime offenses.[7]

It facilitates gathering evidence for investigations and prosecutions of ransomware attacks.

International cooperation:

The Budapest Convention establishes a framework for cooperation between signatories in investigations and prosecutions. This includes:

* Mutual legal assistance (sec16-20)

* Extradition (sec 21-27)

* Joint investigations and procedures (sec 28-30)

This cooperation is crucial for tackling transnational ransomware attacks, where attackers and victims may be located in different countries.

Limitations of the Budapest Convention:

- Limited scope: The Convention doesn't explicitly address ransomware attacks, focusing more on broader cybercrime categories.

- Non-self-executing treaty: Each signatory needs to implement the Convention through national legislation, leading to variations in enforcement across countries.

- **United Nations Convention against Transnational Organized Crime (2000):** This treaty, while broader in scope, recognizes the threat of cybercrime and encourages cooperation in investigations and prosecutions.

[7] Article 16: Search and seizure of computer data ([Council of Europe, Convention on Cybercrime, ETS No. 185, art. 16 (2001)])

While broader in scope, the UNTOC recognizes the threat of cybercrime and encourages cooperation in combating it. Here's how it complements the Budapest Convention:

a) Article 27: Illicit trafficking in information technology products: This article criminalizes the production, acquisition, possession, supply, or use of computer programs designed for the purpose of committing a criminal offense. [8]

It could potentially be used against developers and distributors of ransomware tools.

b) Article 23: Measures against the laundering of proceeds from crime: This article encourages cooperation in tracing, freezing, and confiscating proceeds from crime, including those derived from cybercrime.[9]

It can be helpful in disrupting the financial ecosystem of ransomware attackers who rely on ransom payments.

The Budapest Convention and UNTOC provide a foundation for international cooperation in combating cybercrime, laying the groundwork for addressing ransomware attacks, but further development and refinement are needed for a comprehensive legal framework.

LEGAL PROVISIONS REGARDING RANSOMWARE ATTACKS IN INDIA

The legal and regulatory frameworks addressing ransomware attacks vary across jurisdictions. In the United States, for example, the Computer Fraud and Abuse Act (CFAA) and the Racketeer Influenced and Corrupt Organizations (RICO) Act can be invoked to prosecute ransomware attackers. In India, the Information Technology Act, 2000, and the Indian Penal Code include provisions that can be applied to combat ransomware attacks.India has a developing legal framework to address cybercrime, including ransomware attacks. Here's a breakdown of key legal provisions:

1. The Information Technology Act, 2000 (IT Act):

The IT Act serves as the cornerstone of India's cybercrime legislation. Several provisions are

[8] Article 27: Illicit trafficking in information technology products ([United Nations, Convention against Transnational Organized Crime, art. 27 (2000)])
[9] Article 23: Measures against the laundering of proceeds from crime ([United Nations, Convention against Transnational Organized Crime, art. 23 (2000)])

relevant to ransomware attacks:

- Section 43: Damage to computer, computer system etc. This section criminalizes acts that damage a computer system, data, or disrupt its functioning. Ransomware attacks often involve such actions when attackers encrypt data, rendering it inaccessible.

- Section 66: Hacking and data breach: This section prohibits unauthorized access to a computer system or data. Ransomware attacks typically involve gaining unauthorized access to a victim's system before encrypting data.

- Section 70: Punishment for contravention of Section 43 and 66. This section prescribes penalties for offenses under Sections 43 and 66, including imprisonment and fines.

2. Indian Penal Code, 1860 (IPC):

The IPC, India's primary criminal code, can also be applied to certain aspects of ransomware attacks:

- **Section 425: Mischief:**

This section covers acts intended to cause wrongful loss or damage to property. In some cases, ransomware attacks could be interpreted as mischief causing damage to electronic data.

- **Section 426: Mischief causing damage to property with intent to cause prejudice to any person.**

This section applies when the act of mischief is done with the intention of harming someone. Ransomware attacks often aim to coerce victims into paying a ransom, potentially falling under this provision.

- **Section 406: Punishment for criminal breach of trust.**

This section deals with criminal misuse of property entrusted to someone. In some instances, if a victim entrusts data to a service provider who is then compromised by ransomware, this section might be relevant.

LEGAL CHALLENGES IN COMBATTING RANSOMWARE ATTACKS:

Despite the existing legal provisions, India faces challenges in effectively combating ransomware attacks:

1. Jurisdictional Hurdles:

a) Transnational nature of cybercrime: Ransomware attacks often transcend national borders.[10] Attackers may launch attacks from countries with weak cybercrime laws or limited international cooperation. This makes it difficult to identify perpetrators, gather evidence, and prosecute them.[11]

Limited success has been achieved in prosecuting attackers located abroad. For instance, despite international cooperation efforts, no arrests were made in the high-profile case of the 2017 WannaCry ransomware attack, which affected over 150 countries.[12]

b) Challenges in extradition: Extradition treaties may not cover cybercrimes, or requesting countries may face lengthy and complex procedures to secure the extradition of attackers located abroad.[13]

Case Law:

- USA v. Vinnik, No. 17-cr-185 (N.D. Cal. 2017): Alexander Vinnik was indicted in the United States for operating a digital currency exchange used to launder proceeds from ransomware attacks, highlighting the complexities of jurisdiction in cybercrimes.[14]

Legal Provisions:

- Budapest Convention on Cybercrime, Article 32: Addresses issues related to jurisdiction and international cooperation in cybercrime investigations and prosecutions.[15]

[10] D. Smith, 'Jurisdictional Challenges in Combating Cybercrime' (2019) 25 International Journal of Cybersecurity 112.
[11] Council of Europe, Convention on Cybercrime, ETS No. 185, art. 16-20 (2001)
[12] European Union Agency for Cybersecurity (ENISA), Threat Landscape for Ransomware 2022 (Sept. 2022)
[13] Sam Zuckerberger, et al., A Blueprint for a Comprehensive Approach to Countering Ransomware, The White House (May 11, 2021), https://www.whitehouse.gov/briefing- room/statements-releases/2023/11/01/fact-sheet-biden-harris-administration-convenes-third-global-gathering-to-counter-ransomware/))
[14] USA v. Vinnik, No. 17-cr-185 (N.D. Cal. 2017)
[15] Council of Europe, Budapest Convention on Cybercrime, CETS No.: 185, Article 32.**

2. Anonymity of Attackers:

a) Sophisticated techniques: Attackers often use anonymization tools and techniques like cryptocurrency to conceal their identities and locations. This makes it difficult for law enforcement to trace them and build cases.[16]

In the 2021 attack on Colonial Pipeline, a major US fuel pipeline operator, authorities were unable to identify the attackers definitively, highlighting the difficulty of tracing identities through cryptocurrency transactions.[17]

b) Dark web marketplaces: Attackers frequently operate on dark web marketplaces where they sell ransomware tools and services, further obscuring their identities and activities.

Case Law:

- US v. Ghinkul: Andrey Ghinkul was extradited to the United States and convicted for his involvement in a ransomware scheme, demonstrating the importance of international cooperation in cybercrime investigations.[18]

Legal Provisions:

- United Nations Convention against Transnational Organized Crime, Article 16: Provides for international cooperation in combating transnational organized crime, including cybercrimes.[19]

3. Difficulties in Tracing and Seizing Cryptocurrency Ransom Payments:

a) Pseudonymous nature of cryptocurrency: Cryptocurrency transactions are pseudonymous, making it difficult to identify the ultimate recipient of ransom payments.

Despite recovering some ransom payments in the Colonial Pipeline attack, challenges remain in identifying the ultimate recipients due to the pseudonymous nature of cryptocurrency

[16] Sarah Soubhian, Ransomware Attacks: A Primer on the Legal and Regulatory Landscape, The Lawfare Institute (Sept. 10, 2020), (https://crsreports.congress.gov/product/pdf/R/R46932))
[17] U.S. Department of Justice, Justice Department Recovers Over $2.3 Million in Ransom Paid in Colonial Pipeline Attack (June 7, 2021)
[18] US v. Ghinkul, No. 15-cr-00103 (E.D. Va. 2015)
[19] United Nations Office on Drugs and Crime, United Nations Convention against Transnational Organized Crime, Article 16

transactions.

b) Challenges in international cooperation: Regulations and enforcement capabilities regarding cryptocurrency vary across countries, hindering efforts to track and seize ransom funds.

Strengthening international cooperation through treaties like the Budapest Convention on Cybercrime (2001) is vital for information sharing, investigations, and extradition procedures.[20]

Case Law:

-WannaCry Ransomware Attack (2017): A global ransomware attack that exploited vulnerabilities in outdated software, highlighting the need for updated legal and regulatory frameworks to address evolving cyber threats.[21]

Legal Provisions:

- Information Technology Act, 2000, Section 43: Addresses unauthorized access, downloading, and extraction of data, but may require amendments to specifically address ransomware attacks.[22]

4. Legal and Ethical Considerations of Disrupting Ransomware Operations:

a) Lawful hacking: Law enforcement agencies may consider hacking into ransomware infrastructure to disrupt operations and prevent attacks. This raises legal concerns about exceeding their authority and potentially causing unintended consequences.

b) Sanctions and unintended consequences: Sanctions against cryptocurrency wallets or exchanges associated with ransomware attackers may have unintended consequences, disrupting legitimate uses of cryptocurrency.

5. Challenges in Victim Cooperation:

a) Fear of prosecution: In some cases, victims may hesitate to report ransomware attacks

[20] Council of Europe, Convention on Cybercrime, ETS No. 185, art. 16-20 (2001) [hereinafter Budapest Convention])
[21] M. Gupta, 'WannaCry Ransomware Attack and Legal Implications' (2018) 20 Journal of Indian Cyber Law 34
[22] Information Technology Act, 2000, No. 21, Acts of Parliament, 2000 (India), Section 43

due to fear of prosecution if their data contained sensitive information or violated regulations.

b) Pressure to pay ransom: Victims facing data loss or operational disruption may feel pressured to pay ransoms, hindering investigations and emboldening attackers.

6. Evolving Nature of Ransomware:

Emerging tactics: Ransomware attackers continuously develop new techniques, such as double extortion (stealing data before encryption) and targeting critical infrastructure. This necessitates constant adaptation of legal frameworks and enforcement strategies.

THE STEPWISE PROCESS OF RANSOMWARE ATTACK:

Step 1: Initial Infection

A. Delivery of Malicious Payload[23]

- Phishing Emails: The most common method of initial infection is through phishing emails containing malicious attachments or links.
- Malicious Website: Visiting compromised or malicious websites can also lead to the download and execution of ransomware.
- Exploiting Vulnerabilities: Cybercriminals exploit software vulnerabilities to deliver ransomware using exploit kits.

B. Execution of Malicious Payload:

- Activation: Once the malicious payload is executed, the ransomware starts its malicious activities, such as encrypting the victim's files or locking the victim out of their device.

[23] I've Been Hit By Ransomware! https://www.cisa.gov/stopransomware/ive-been-hit-ransomware

Step 2: Encryption of Victim's Data

A. Scanning and Identification

- File Scanning: The ransomware scans the victim's device for targeted files to encrypt, such as documents, photos, and databases.
- Encryption Process: The ransomware encrypts the targeted files using strong encryption algorithms, making them inaccessible to the victim.[24]

B. Displaying Ransom Note

- Ransom Note: After encrypting the victim's data, the ransomware displays a ransom note on the victim's screen, providing instructions on how to pay the ransom to decrypt the files.

Step 3: Ransom Demand

A. Payment Instructions:

- Cryptocurrency Payment: The attacker provides instructions for making the ransom payment, usually in cryptocurrency like Bitcoin, to receive the decryption key or restore access to the compromised device or data.

B. Threat of Data Loss or Disclosure

- Data Exfiltration: In some cases, the ransomware attackers may threaten to publish or sell the victim's data if the ransom is not paid, adding a layer of extortion to the attack.

C. Time-sensitive Demands

- Deadline for Payment: The attacker imposes a deadline for the ransom payment, adding urgency and pressure on the victim to comply with the attacker's demands.

[24] From Infiltration to Execution: Understanding the Phases of a Ransomware Attack, https://www.linkedin.com/pulse/from-infiltration-execution-understanding-phases-ransomware-attack

Step 4: Payment and Decryption

A. Payment Verification

- Payment Confirmation: After receiving the ransom payment, the attacker verifies the payment and provides the decryption key to the victim.[25]

B. Decryption Process

- Decryption Key: The victim uses the provided decryption key to decrypt their files and restore access to their data or device.

Step 5: Post-Attack Recovery and Prevention

A. Data Restoration

- Data Recovery: The victim restores their encrypted files using the decryption key provided by the attacker or through data backup and recovery processes.

B. Security Measures and Prevention

- Security Updates: Updating and patching software and systems to prevent future vulnerabilities and exploits.

- Security Awareness Training: Educating individuals and organizations about cybersecurity best practices, including recognizing phishing emails and avoiding malicious websites.

The stepwise process of a cyber ransomware attack involves initial infection through the delivery of a malicious payload, encryption of the victim's data, demand for ransom payment, payment and decryption, and post-attack recovery and prevention measures. Understanding this process is crucial for enhancing awareness, prevention, and response strategies to combat ransomware attacks effectively and mitigate the risks and impacts of this form of cybercrime.

[25] National cyber security center, Mitigating malware and ransomware attacks, https://www.ncsc.gov.uk/guidance/mitigating-malware-and-ransomware-attacks

INTERNATIONAL CASE LAWS RELATED TO RANSOMWARE ATTACKS:

1. ***WannaCry Ransomware Attack (2017)***

The WannaCry ransomware attack occurred in May 2017 and was a global cyberattack that affected over 200,000 computers in 150 countries. The ransomware encrypted data on the computers and demanded ransom payments in Bitcoin from the victims to decrypt their data.

2. US v. Mihai Alexandru Isvanca & Eveline Cismaru (2018)

Mihai Alexandru Isvanca and Eveline Cismaru were indicted in the United States for their involvement in the distribution of ransomware, including Winlocker. The ransomware targeted victims in the United States, encrypting their data and demanding ransom payments.

The case was prosecuted in the Eastern District of Virginia. Mihai Alexandru Isvanca and Eveline Cismaru faced charges related to conspiracy to commit wire fraud, conspiracy to commit fraud and related activity in connection with computers, and conspiracy to commit money laundering. Both defendants were extradited to the United States to face prosecution.

3. State of Utah v. Alexander Filinov (2020)

Alexander Filinov was charged in the state of Utah for his involvement in the distribution of Maze ransomware. The Maze ransomware not only encrypted the victims' data but also threatened to publish the data if the ransom was not paid, adding a layer of extortion to the attack.

Alexander Filinov faced charges related to computer crimes and extortion. The case highlighted the increasing complexity and sophistication of ransomware attacks, as well as the extortionate tactics used by ransomware attackers.

4. US v. Yaroslav Vasinskyi (2021)

Yaroslav Vasinskyi was charged in the United States for his involvement in the distribution of Sodinokibi (REvil) ransomware as part of a Ransomware as a Service (RaaS) scheme. The RaaS model allows cybercriminals to lease or sell ransomware to other criminals to conduct ransomware attacks.

Yaroslav Vasinskyi faced charges related to conspiracy to commit fraud and related activity in connection with computers and conspiracy to commit money laundering. The case highlighted the evolution of ransomware attacks and the role of Ransomware as a Service in facilitating and proliferating ransomware attacks.

5. NHS Cyber Attack (2017)

A ransomware attack targeted the UK's National Health Service (NHS) in 2017, causing significant disruption to healthcare services. The ransomware encrypted data on NHS computers and demanded ransom payments from the NHS to decrypt their data and restore their systems.

6. Atlanta Ransomware Attack (2018)

A ransomware attack targeted the city of Atlanta, Georgia, in 2018, disrupting city services and illustrating the impact of ransomware attacks on municipal governments and critical services. The ransomware encrypted data on the city's computers and demanded ransom payments to decrypt their data and restore their systems.

7. Garmin Ransomware Attack (2020)

A ransomware attack targeted Garmin, a multinational technology company, in 2020, causing significant disruption to its online services. The ransomware encrypted data on Garmin's computers and demanded ransom payments from Garmin to decrypt their data and restore their systems.

INSTANCES OF RANSOMWARE ATTACKS IN INDIA

- **Kochi Metro Rail Limited Ransomware Attack (2019)[26]**

In 2019, Kochi Metro Rail Limited (KMRL) in Kerala, India, suffered a ransomware attack that affected its operations and computer systems. The ransomware encrypted data on KMRL's computers and demanded a ransom payment to decrypt the data and restore the systems. The

[26] https://timesofindia.indiatimes.com/city/kochi/cyber-attack-downs-kochi-metro-website/articleshow/19452606.cms

attack disrupted the metro rail services and posed significant operational and financial challenges for KMRL.

- **Tamil Nadu Electricity Board Ransomware Attack (2020)**

In 2020, the Tamil Nadu Electricity Board (TNEB) in Tamil Nadu, India, experienced a ransomware attack that impacted its operations and computer systems. The ransomware encrypted data on TNEB's computers and demanded a ransom payment to decrypt the data and restore the systems. The attack disrupted the electricity distribution and billing services of TNEB, causing inconvenience to the consumers and financial losses to the board.[27]

- **Andhra Pradesh State Road Transport Corporation Ransomware Attack (2021)**

In 2021, the Andhra Pradesh State Road Transport Corporation (APSRTC) in Andhra Pradesh, India, was targeted by a ransomware attack that affected its operations and computer systems. The ransomware encrypted data on APSRTC's computers and demanded a ransom payment to decrypt the data and restore the systems. The attack disrupted the bus services and online ticketing system of APSRTC, causing inconvenience to the passengers and financial losses to the corporation.[28]

- **Maharashtra Industrial Development Corporation Ransomware Attack (2018)**

In 2018, the Maharashtra Industrial Development Corporation (MIDC) in Maharashtra, India, fell victim to a ransomware attack that impacted its operations and computer systems. The ransomware encrypted data on MIDC's computers and demanded a ransom payment to decrypt the data and restore the systems. The attack disrupted the industrial development and business operations of MIDC, causing financial losses and posing security concerns for the industrial sector in Maharashtra.[29]

[27] Tamil Nadu Public Department comes under ransomware attack
Sensitive documents encryptedhttps://www.thehindu.com/news/national/tamil-nadu/tn-public-dept-attacked-by-ransomware-sensitive-documents-encrypted/article36531408.ece
[28] Ransomware attack: Andhra Pradesh police, firms hit; CERT issues advisory, https://www.business-standard.com/article/current-affairs/ransomware-attack-andhra-pradesh-police-firms-hit-cert-issues-advisory-117051300845_1.html
[29] Ransomware attack on MIDC server: Attack origin traced to Russia-Kazakhstan, https://www.hindustantimes.com/cities/mumbai-news/ransomware-attack-on-midc-server-attack-origin-traced-to-russiakazakhstan-101617911928707.html

- **Indian Banking Sector Ransomware Attacks (Multiple Cases)**

Several banks and financial institutions in India have been targeted by ransomware attacks over the years, impacting their operations and customer data. The ransomware encrypted data on the banks' computers and demanded ransom payments to decrypt the data and restore the systems. The attacks disrupted the banking services, online transactions, and customer services of the banks, causing inconvenience to the customers and financial losses to the banking sector in India.

- **State (NCT of Delhi) v. Ankit Saxena (2018**

This case involved a hacking incident where the accused allegedly gained unauthorized access to a computer system and altered data. While not explicitly a ransomware attack, the unauthorized access and data manipulation bear similarities to some ransomware tactics.

The Delhi High Court convicted the accused under Section 66 of the Information Technology Act, 2000 (IT Act) for hacking and data alteration. This case demonstrates the potential application of the IT Act to address unauthorized access to computer systems, a key element in many ransomware attacks.[30]

- **Vijay Shankar v. State (2020)**

This case involved a phishing attack where the accused allegedly sent emails impersonating a bank to trick the victim into revealing confidential information. While not directly related to ransomware, phishing attacks are often used by cybercriminals to gain access to systems that could then be targeted by ransomware.

The Kerala High Court upheld the conviction of the accused under Section 66D of the IT Act for cheating by personation using a computer resource. This case highlights the potential use of the IT Act to address cyber deception tactics that could be employed as precursors to ransomware attacks.[31]

[30] State (NCT of Delhi) v. Ankit Saxena, FAO(OS) 1169/2017 (Delhi High Court 2018)
[31] Vijay Shankar v. State, W.P.(Crl.) No. 3317 of 2019 (Kerala High Court 2020)

CONCLUSION

The international legal framework provides a foundation for cooperation, but it needs further development to address the evolving tactics and challenges of these attacks. While India has existing cybercrime legislation, it can be strengthened through targeted legislation, enhanced investigative powers, and clarity on cryptocurrency regulations. Additionally, international cooperation, public awareness campaigns, and improved cybersecurity practices are crucial for mitigating ransomware threats.

By implementing the recommendations outlined in this paper, India can build a more robust legal framework and enhance its cybersecurity posture. This calls for a collaborative effort from government, law enforcement agencies, the private sector, and the public to create a more secure digital environment for all.

SUGGESTIONS AND RECOMMENDATIONS

1. Strengthening Legal Framework

a. Specific Legislation on Cyber Ransomware Attacks:

Recommendation: Introduce specific legislation addressing cyber ransomware attacks to define the offense, penalties, and legal procedures. Consider enacting specific legislation addressing ransomware attacks. This legislation could define ransomware, outline offenses and penalties, and provide for victim support and restitution mechanisms.

b. Harmonization with International Standards:

Recommendation: Align the Indian legal framework with international standards and conventions on cybersecurity and cybercrime.

Harmonization with international standards will enhance international cooperation, information sharing, and collaboration in combating cyber ransomware attacks.

c. Enhancement of Law Enforcement Capabilities

Recommendation: Strengthen the capabilities and training of law enforcement agencies to investigate and prosecute cyber ransomware attacks effectively.

Improving the capabilities of law enforcement agencies will enhance the detection, investigation, and prosecution of cyber ransomware attacks, ensuring justice for the victims.

2. Improving Cybersecurity Measures

a. Implementation of Robust Cybersecurity Measures

Recommendation: Implement robust cybersecurity measures, including advanced threat detection, incident response, and recovery plans to prevent and mitigate cyber ransomware attacks.

Effective cybersecurity measures are essential to prevent cyber ransomware attacks and minimize the impact on critical infrastructure and businesses.

b. Regular Cybersecurity Audits and Compliance Checks

Recommendation: Conduct regular cybersecurity audits and compliance checks for organizations, businesses, and critical infrastructure to assess and improve their cybersecurity posture.

Regular cybersecurity audits and compliance checks will identify vulnerabilities, weaknesses, and non-compliance with cybersecurity standards, facilitating timely remediation and improvement.

c. Public Awareness and Education on Cybersecurity

Recommendation: Enhance public awareness and education on cybersecurity best practices, including ransomware prevention, detection, and response strategies.

Increasing public awareness and education on cybersecurity will empower individuals, organizations, and businesses to adopt cybersecurity best practices and protect themselves against cyber ransomware attacks.

3. Encouraging International Cooperation and Collaboration

a. International Cooperation and Information Sharing

Recommendation: Strengthen international cooperation and information sharing mechanisms

with other countries, international organizations, and cybersecurity agencies to combat cyber ransomware attacks effectively.

International cooperation and information sharing are essential to identify, track, and prosecute cyber ransomware attackers operating across borders, enhancing the global cybersecurity ecosystem.

b. Participation in International Cybersecurity Initiatives and Forums

Recommendation: Actively participate in international cybersecurity initiatives, forums, and collaborative platforms to share knowledge, best practices, and resources on combating cyber ransomware attacks.

Participation in international cybersecurity initiatives and forums will enhance India's cybersecurity capabilities, knowledge sharing, and collaboration in addressing cyber ransomware attacks at a global level.

4. Strengthening Incident Response and Recovery Mechanisms

a. Development of National Cyber Incident Response Plan

Recommendation: Develop a national cyber incident response plan outlining the roles, responsibilities, and procedures for responding to cyber ransomware attacks and coordinating with relevant stakeholders.

A national cyber incident response plan will facilitate coordinated and effective response to cyber ransomware attacks, minimizing the impact and ensuring swift recovery.

b. Enhancement of Cyber Insurance Policies

Recommendation: Encourage the adoption and enhancement of cyber insurance policies by organizations, businesses, and critical infrastructure to mitigate the financial impact of cyber ransomware attacks.

Cyber insurance policies will provide financial protection and support organizations, businesses, and critical infrastructure in recovering from cyber ransomware attacks and managing the associated costs and liabilities.

5. Collaboration with the Private Sector:

a. Public-Private Partnerships: Foster public-private partnerships to leverage expertise from the private sector in developing cybersecurity solutions and sharing threat intelligence.

b. Information Sharing Platform: Create a secure information sharing platform between law enforcement agencies and the private sector to facilitate timely threat alerts and coordinated responses.

REVIEW OF LITERATURE

A) In the article 'It's more than just money: The real-world harms from ransomware attacks' [32] the study offers a fresh perspective on the various real-world damages stemming from cyber-attacks, emphasizing ransomware incidents. Utilizing publicly-accessible case data on prominent ransomware attacks, the researchers scrutinize the kinds of damage that manifest at different stages post-attack.

The study introduces an innovative methodology for assessing damages from ransomware incidents, utilizing directed graphs to visually depict the connections between different types of harm. The examination uncovers a significant array of social and human-related damages beyond just the business impact and reveals a convoluted network of damages that arise following attacks, irrespective of the industry sector.

Due to the limited availability of comprehensive data, determining the complete scope and sequence of damages remains a complex endeavor. The study advocates for increased transparency regarding the damages caused by ransomware to gain a better understanding of the realities associated with these incidents.

B) In the article 'Ransomware-based Cyber Attacks: A Comprehensive Survey"[33] the study examines the security and privacy challenges in IoT devices, attributing them to inadequate security design and the diversity of IoT devices. It underscores the

[32] It's more than just money: The real-world harms from ransomware attacks 06 Jul 2023
[33] Ransomware-based Cyber Attacks: A Comprehensive Survey, 01 Dec 2022-Journal of Internet Technology (Journal of Internet Technology)-Vol. 23, Iss: 7, pp 1557-1564

growing adoption of IoT devices across various sectors, including Smart Homes, Smart Farming, and Smart Enterprises

The authors present potential service scenarios for detecting ransomware-based cyber-attacks in IoT and highlight ongoing research challenges and future prospects related to ransomware in IoT The study outlines the impacts of ransomware-based cyber-attacks, encompassing data loss, disruption of system operations, and financial repercussions. It delves into the two primary categories of ransomware, namely cryptoransomware and locker ransomware

The research focuses on the security and privacy challenges tied to the detection of Ransomware-based Cyber Attacks in IoT applications. It contrasts current research and development efforts concerning key technologies, application environments, and methodologies

The study underscores the dynamic nature of ransomware attacks targeting IoT devices in smart cities and points out the challenges arising from the limited computational capabilities of devices and the absence of a consistent security framework

The authors acknowledge the support provided by the Future Challenge Defense Technology Research and Development Project for this research.

C) **In the article 'Ransomware Attacks in History of Cyber World' authored by Fizza Zafri[34] The study offers an in-depth examination of the history of ransomware attacks in the cyber realm, with the objective of enlightening students and enhancing forensic awareness.**

It explores the expansion of internet technology and devices, which have escalated the vulnerability to cyber attacks, thus making cybersecurity a crucial topic in forensic science.

The study delves into various facets of ransomware attacks, elucidating their nature, functioning, and evolution over the years

It underscores the significance of familiarizing oneself with past attacks for students of forensic

[34] Fizza Zafri, Ransomware Attacks in History of Cyber World, 31 Jan 2022-International Journal For Science Technology And Engineering-Vol. 10, Iss: 1, pp 39-43

science and provides insights into preventing ransomware attacks

The research emphasizes the imperative for organizations and individuals to take a proactive approach in safeguarding against ransomware attacks by staying abreast of the latest developments and implementing security protocols.

It references the inaugural documented case of a ransomware attack in the cyber world, wherein a researcher disseminated infected floppy disks to AIDS researchers. The study concludes by advocating for regular data backups, timely device and software updates, and staying informed about emerging ransomware threats as precautionary measures.

REFERENCES:

ARTICLES:

- It's more than just money: The real-world harms from ransomware attacks 06 Jul 2023
- Ransomware-based Cyber Attacks: A Comprehensive Survey, 01 Dec 2022-Journal of Internet Technology (Journal of Internet Technology)-Vol. 23, Iss: 7, pp 1557-1564
- Fizza Zafri, Ransomware Attacks in History of Cyber World, 31 Jan 2022-International Journal for Science Technology and Engineering-Vol. 10, Iss: 1, pp 39-43

LEGISLATIONS:

- National Cybersecurity Strategy, Ministry of Electronics and Information Technology, Government of India (2020).
- Budapest Convention on Cybercrime, Council of Europe (2001).
- Cyber Crime Investigation Manual, Central Bureau of Investigation, Government of India (2019).
- Cybersecurity Framework, National Institute of Standards and Technology, U.S. Department of Commerce (2018).
- Cybersecurity Guidelines and Best Practices, Reserve Bank of India (2021).
- Cybersecurity Awareness and Education Programs, Cyber Swachhta Kendra, Ministry of Electronics and Information Technology, Government of India (2021).
- International Cooperation on Cybersecurity, United Nations Office on Drugs and Crime (2020).
- Participation in International Cybersecurity Initiatives and Forums, Ministry of External Affairs, Government of India (2021).
- National Cyber Incident Response Plan, Cyber Coordination Centre, Ministry of Home

Affairs, Government of India (2020).

- Cyber Insurance Policies and Guidelines, Insurance Regulatory and Development Authority of India (2021).

WEBLIOGRAPHY

- https://www.cisa.gov/stopransomware/ive-been-hit-ransomware
- https://www.linkedin.com/pulse/from-infiltration-execution-understanding-phases-ransomware-attack
- National cyber security center, Mitigating malware and ransomware attacks, https://www.ncsc.gov.uk/guidance/mitigating-malware-and-ransomware-attacks
- https://www.kaspersky.co.in/resource-center/threats/ransomware-attacks-and-types
- https://www.crowdstrike.com/cybersecurity-101/ransomware/types-of-ransomware/
- https://www.checkpoint.com/cyber-hub/threat-prevention/ransomware/
- https://www.ibm.com/topics/ransomware
- https://www.cyber.gov.au/threats/types-threats/ransomware
- https://timesofindia.indiatimes.com/city/kochi/cyber-attack-downs-kochi-metro-website/articleshow/19452606.cms
- https://www.thehindu.com/news/national/tamil-nadu/tn-public-dept-attacked-by-ransomware-sensitive-documents-encrypted/article36531408.ece
- https://www.business-standard.com/article/current-affairs/ransomware-attack-andhra-pradesh-police-firms-hit-cert-issues-advisory-117051300845_1.html
- https://www.hindustantimes.com/cities/mumbai-news/ransomware-attack-on-midc-server-attack-origin-traced-to-russiakazakhstan-101617911928707.html