

VOL. I/ISSUE I/2024



A PAVAN DUGGAL ASSOCIATES INITIATIVE

INTERNATIONAL JOURNAL ON CYBERLAW, CYBERCRIME & CYBERSECURITY

WWW.PAVANDUGGALASSOCIATES.COM

S.NO.	NAME OF ARTICLE	PAGE NO.	DETAILS OF AUTHOR(S)
1.	<u>AIIMS RANSOMWARE ATTACK: A WAKE-UP CALL FOR INDIA</u>	Page 03- Page 04	Dr. Pavan Duggal Advocate, Supreme Court Of India President, Cyberlaws.Net S-307, Block S, Part 1, Greater Kailash, New Delhi, Delhi 110048 + 91 11 4658 4441 pavanduggal@yahoo.com

AIIMS RANSOMWARE ATTACK: A WAKE-UP CALL FOR INDIA

The recent AIIMS attack has been in the news lately. As per the information in the public domain, AIIMS got hit by a massive ransomware attack which completely disabled all its digital services. As per reports, the entire data has been encrypted, is not accessible and the hackers have demanded 200 crores as ransom. As a result, all cards are being made manually as per information in the public domain.

This represents the biggest ransomware attack till date in the Indian history on Indian health ecosystem. The very fact that cyber criminals have targeted AIIMS is not surprising. The reason is that AIIMS represents one of the most premier medical institution in the country. Further, it has the medical data of all Ministers, politicians, bureaucrats, governmental officers, thought leaders apart from the common citizens of India.

With so much quantum of data gone and services still paralysed, the question that comes up for consideration is where we are standing and what we need to do as a nation. The reality is that India is not at all well equipped to deal with any kinds of ransomware attacks. The reasons for this is not far to find. India till date has provided lip-service to all aspects of cyber security. This is all the more so as India does not have dedicated law on cyber security. India also does not have dedicated law on ransomware.

The National Cyber Security Policy 2013 is mere a paper-tiger and has not been implemented. India is still working on the draft of the National Cyber Security Strategy but the said Strategy has still not been released.

Further, the Information Technology Act, 2000 is not a cyber security legislation, though, it has defined cyber security in legal terms. It needs to be noted that the Information Technology Act, 2000 as amended, has made cosmetic provisions on cyber security. It needs to be appreciated that with the advent of Covid-19, the Golden Age of Cybercrime has arrived.

Indian installations including Indian Critical Information Infrastructures are vulnerable in terms of their security preparedness. That is the reason why institutions like AIIMS have been attacked with such ease by cyber attackers.

India needs to treat the AIIMS ransomware attack as a wakeup call so that it needs to wake up from its deep slumber. India needs to give dedicated focus on cyber security. There is a crying need for India to have dedicated law on cyber security. The onus is on the Government on how it comes up with appropriate mechanisms for protection and preservation of cyber security today.

Even from the perspective of the Indian nation as a whole, cyber security has to attain more significance and relevance in our day-to-day lives. Digital users need to understand that we are all links in a big cyber security chain and the cyber security chain of our nation is as strong as a weakest link, therefore we have to make sure that we do not become the weakest link of the cyber security chain.

We also need to ensure that we have to start adopting cyber security as a way of life. We should not expect cyber security only as the governmental responsibility. On the other hand, we all need to contribute towards making cyber security of a nation more secure.

Cyber security is a constantly evolving paradigm and constantly moving target. India would serve its national interest not far better if it has a dedicated Ministry on cyber security.

Creating more awareness about cyber security amongst digital users will also be an important ongoing phenomenon. Users will have to keep on making their devices, computers and laptops more secure and use appropriate firewalls, antivirus and appropriate protection in this regard. Individuals must not be reckless while sharing their information online.

We need to realize that we need to share information only on a need-to-know basis. We must have regular backups of our systems and accounts so that in the event we become a victim of a ransomware attack, we can try to restore data from our backups and assume normalcy.

We must also be studiously careful not to click on any outside link provided by third parties or disclose confidential information including our bank details and sensitive personal data. We have to be cautious, careful and constantly diligent all the times. Constant vigil is the price that we have to pay for having in place a secure and reliable cyberspace.

Hopefully, the AIIMS ransomware attack could shake India out of its deep slumber and propel the Indian nation to work as a holistic unit to deal with the emerging challenges of ransomware and increasing cyber security breaches with each passing day.

The author Dr. Pavan Duggal, Advocate, Supreme Court of India, is an internationally renowned expert authority on Cyberlaw and Cybersecurity law. He has been acknowledged as one of the top four Cyber lawyers in the world. He is the Honorary Chancellor of Cyberlaw University and also the Chairman of International Commission on Cybersecurity Law. You can reach him at pavan@pavanduggal.com. More about Dr. Pavan Duggal is available at www.pavanduggal.com.