Lucknow Law Review

Short Article

The Plague of Ransomware and Cyber-Attacks: Challenges and the Road Ahead

Sean McDonald[1]

[1] *School of Law, Narsee Monjee Institute of Management Studies, Bengaluru*

Published on: September 1, 2021
Page No.: 60 – 68
Manuscript No.: 2021/LNLR/01060
Editors: Adnan Athar Quraishi, Mohd Rameez Raza

Cite as: Sean McDonald, The Plague of Ransomware and Cyber-Attacks: Challenges and the Road Ahead (2021) 1(2) LKO. L. REV. 60

Find here: *https://www.lucknowlawreview.org/sean-mcdonald*

Abstract: *Cyber and ransomware attacks across the globe have been a troubling issue faced by Governments and Companies alike. Crucial systems are encrypted and personal data of consumers are breached by hackers. Victims are forced to pay massive amounts in ransom in cryptocurrency to recover these systems. Data of consumers finds its way to the dark web which ransomware attacks through the lens of the recent Colonial Pipeline incident, the aftermath of which opens up a sea of further consequences. This article explores the concept of rah created some interesting outcomes which might depict a way to proactively target the perpetrators of these attacks. The article also highlights the prevailing situation in India with regards to ransomware attacks and data breaches and analyses the situation from a legal perspective looking at both the current IT rules governing data breaches, the roles and functions of the nodal agency CERT-In and the possible changes that we can expect with the incoming Personal Data Protection Bill, 2019 regarding questions of reporting data breaches, penalties and steps to mitigate damage. The author suggests the shortcomings and changes required to build a better framework. As a conclusion, the author calls for a two-pronged approach consisting of proactive targeting by agencies to monitor and apprehend the perpetrators of these attacks as well as strong framework to tackle and mitigate damage in the event of a breach/attack.*

Keywords: *Ransomware, Data Breach, Legal Consequences, Data Protection.*

1. Introduction

Over the last couple of months, ransomware attacks by hackers on critical global infrastructure such as oil, healthcare, manufacturing and food processing etc. has taken center stage as the scale and level of sophistication employed by hackers in these incidents have increased several folds wreaking havoc and depicting a troubling picture for most enterprises. When malicious code is used to deny/restrict a user or organization access to a computer system or data, it is known as a ransomware cyber-attack. The malware is usually disseminated by hackers through phishing emails or visits to malicious websites. In return hackers demand a ransom to unlock these crucial systems.

Just in 2021, across the globe there has far too many reported incidents of prominent ransomware attacks on major companies. These incidents are reported because of the level of impact on reputed companies and scale of the operation. There are most likely to be unreported incidents that far surpass the number of reported ones. While the US has been bearing the brunt of these attacks, the rest of the world too have been targeted. Public Schools such as Buffalo Public School, Saginaw Township Community Schools, University of California etc. Washington's Metropolitan Police Department and other police departments, Colonial Pipeline which is the largest fuel pipeline in the US, JBS foods which is the world's largest meat processing firm, Japanese firms such as Hoya, Yamabiko, Toyota etc. Healthcare systems such as Scripps and several Health Boards and Hospitals and Indian firms like Upstox and even the Maharashtra Industrial Development Corporation (MIDC) are just few examples.[1] All these include just a fraction of the ransomware attacks that took place over the course of the last 6 months.

The repercussions were astounding, ransoms were demanded to the tune of millions of dollars and critical infrastructure took a big hit. Hospitals were forced to shut down and redirect patients, several firms delivering key products too had to shut down and these triggered shortages like in the case of JBS and Colonial Pipeline and in many instances sensitive personal data of consumers found its way in the dark web when demands weren't met. Loss of such sensitive personal information opens up a sea of further consequences for consumers and the onus falls on the company or the data fiduciary to take the necessary steps to protect the data at all costs. Several hacking groups such as Ryuk, DarkSide, Clop etc. have popped up claiming rights over these incidents and what this signal is growing underground industry promulgating ransomware as a service. These hackers develop code that locks up systems and outsource this malicious code to people willing

[1] 'The State of Ransomware in 2021' (*Black Fog*, 1 June 2021) <https://www.blackfog.com/the-state-of-ransomware-in-2021/>

to use it to conduct these attacks. These people then are responsible for collecting the ransom and share a small price of it with the original hackers. This portrays a wide-reaching conglomerate network capable of infiltrating systems across the globe. This poses a dangerous threat requiring careful cognizance by both Governments and Corporations alike. Recently, the aftermath of the Colonial Pipeline incident resulted in some interesting outcomes that could be beneficial in tackling these ransomware attacks and requires a close understanding.

2. The Colonial Pipeline Incident

Founded in 1962 and headquartered in Alpharetta, Georgia, privately-held Colonial Pipeline is one of the largest pipeline operators in the United States, supplying around 45% of the fuel on the East Coast, including gasoline, diesel, home heating oil, as well as jet fuel etc. Last month, a hacker group named DarkSide unleashed a ransomware attack on the company and as soon as they realized they were under attack, they were forced to shut down operations and look at the kind of damage they were dealing with. But soon, this temporary disruption gave way for fuel shortages across many parts of the US. Concerns about a supply bottleneck pushed gasoline futures to their highest level in three years and the Government had to declare a State of emergency in 17 States. The CEO despite advice against it went ahead and paid the $4.4 Million ransom as they were not sure just how many systems were compromised.[2] The company paid the ransom in Bitcoin. This Bitcoin would have eventually been laundered through several cryptocurrency wallets.

However, recently Authorities recovered what is a portion of the ransom that was paid through cryptocurrency to the perpetrators of the ransomware attack. Investigators seized about 64 bitcoins, valued at roughly $2.3 million, from a virtual wallet. The money has been recovered by the recently launched Ransomware and Digital Extortion Task Force created for the purposes of tackling the "epidemic" of ransomware attacks dubbed as a National Security threat in the US.[3] Despite this being a monumental first step in combatting this threat, there remain some unanswered questions.

[2] Colin Eaton & Dustin Volz, 'Colonial Pipeline CEO Tells Why He Paid Hackers a $4.4 Million Ransom' (*The Wall Street Journal*, 19 May 2021) <https://www.wsj.com/articles/colonial-pipeline-ceo-tells-why-he-paid-hackers-a-4-4-million-ransom-11621435636>

[3] Dustin Volz, Sadie Gurman & David Uberti, 'U.S. Retrieves Millions in Ransom Paid to Colonial Pipeline Hackers' (*The Wall Street Journal*, 7 June 2021) <https://www.wsj.com/articles/u-s-retrieves-millions-paid-to-colonial-pipeline-hackers-11623094399>

According to court filings in the Colonial Pipeline case, the FBI gained access by employing the encryption key associated with the Bitcoin account to which the ransom money was sent.[4] Officials, on the other hand, have not revealed how they obtained the key.

2.1. Analysis

Cryptocurrency is the fuel that hackers use to sustain these ransomware attacks. Cryptocurrencies for all the same reasons that they are lauded for such as decentralized nature and private transactions is also the very same reasons it is perfectly tailored for these sorts of nefarious activities. Cryptocurrencies are relatively more difficult to track and much easier to transfer.

So basically, how this works is that cryptocurrency is based on the principle of pseudonymity which is a state of near anonymity. A Bitcoin wallet is basically your digital secured address consisting of a cryptographic key to carry your cryptocurrency all the while keeping your identity safe. On the other hand, cryptocurrency transactions take place using blockchain through a decentralized network and acts as a public ledger for these transactions. These transactions can be tracked through this network, however the identity of the sender or the receiver will not be revealed. A cryptocurrency transaction takes place by using two keys, a public and a private key. A public key is used to identify a bitcoin wallet for transfer and hence is available publicly and a private key is used to transfer and unlock funds and hence is to be securely protected. The FBI leveraged both of these keys to recover the partial ransom. Through the public key they were able to track the wallets even if the funds were split up in order to launder the money. However, there is no explanation as to how they got hold of the private key in order to transfer the money to themselves.

There are few speculations that can be made as to how this came to be:

1. One possibility is that the FBI leveraged it through collaboration with crypto exchanges as the account was active and the exchange would have the private key of the account.

2. A second possibility is that someone connected to the attack alerted the FBI. This would have been the whole process a lot easier.

[4] Vanessa Romo, 'How A New Team Of Feds Hacked The Hackers And Got Colonial Pipeline's Ransom Back' (*NPR*, 8 June 2021) <https://www.npr.org/2021/06/08/1004223000/how-a-new-team-of-feds-hacked-the-hackers-and-got-colonial-pipelines-bitcoin-bac>

3. The third and most difficult speculation is that the FBI recovered the private key through some measure of hacking or forensics.

Whichever may be true, but one thing we can say for certainty is that this shows the first step to the Government's strategy is to go after the ecosystem that fuels the extortion attacks. Going after the money has always been the traditional approach and the same has been adopted in the case of cryptocurrencies. However, this incident cannot be considered as the one stop solution to retrieving cryptocurrency ransoms. There is no guarantee this can be repeated and even so the best outcome of this incident was that only half the ransom was recovered. Nonetheless, the approach works on mapping out these ransomware attacks and link them to possible targets and should definitely be adopted to track the flow of funds and keep a watch on suspicious wallets. FBI has stated that they are currently tracking over 100 variants of ransomware.[5] This represents a targeted approach by law enforcement agencies in tracking specific transactions and actors in this ransomware space.

In the US there has been a bolstered effort taken to tackle ransomware and other cyber-crimes. Specialized teams are being formed to tackle these attacks. The Biden administration has created a new role within the National Security Council, which is a Deputy National Security Advisor who specializes in cyber security and emerging technology as well as a National Cyber Director under the National Defense Authorization Act to work alongside Congress and the private sector to oversee Government response and Policy Output in this area. Last month, the Biden Administration unveiled an executive order mostly geared towards Federal contractors which makes it mandatory for these developers and contractors to report any such cyber incident that occurs.[6]

3. Cyber Attacks in India: Need for a Pro-Active Approach

If we take a look, apart from a host of ransomware attacks, India has also faced numerous data breaches such as those that hit Big Basket, Just Pay, Unacademy, Big Basket and Dr. Reddy's etc. India, along with the United States, the United Kingdom, Singapore, and Ukraine, was part of the top five cyber-targeted countries in the

[5] 'FBI says it is investigating about 100 types of Ransomwares – WSJ' (Reuters, 4 June 2021) <https://www.reuters.com/technology/fbi-says-it-is-investigating-about-100-types-ransomware-wsj-2021-06-04/>

[6] Executive Order on Improving the Nation's Cybersecurity, (*The White House*, 12 May 2021) <https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/>

world in 2019, with India holding the top spot for three months.[7] India is one of the most cyber-attacked countries in the world, thus stricter cybersecurity and data protection legislation are required to prevent data theft and cybercrime. It's not surprising really, with India's massive consumer base of internet users amounting to half a billion. Over 55% of firms paid a ransom to recover their data, indicating the seriousness of the cyber-attack. Indian organizations have suffered costs of around Rs. 8.02 crore to remedy the damage of every ransomware hack.[8] Another gloomy highlight emphasized the fact that only 8% of victims were capable to prevent the attack before their data was encrypted, in comparison to a global average of 24%, according to a report by Sophos.[9]

Preventing cyber-attacks requires a preventive framework and quick response. The Indian Computer Emergency Response Team (CERT-In) is the government's nodal organization for cyber-threats such as hacking and phishing. Timely reporting of such attacks can go a long way in mitigating the damage caused. The Information Technology (The Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rule, 2013 ("Rules") provide for mandatory reporting of certain types of Cyberattacks to CERT-In which remains functioning on 24-hour basis on all days of the year.[10] The function of CERT-In is to interact with and seek assistance from various stakeholders defined under Rule 10 of the Rules to collect, share and disseminate information and also to respond and prevent cyber security incidents.

The Rules create an important first step towards countering the attacks but lack clarity on several issues. Firstly, the types of attacks mentioned in the annexure of the rules such as 'spoofing' or 'phishing' lack definitions. Further, certain phrases such as "compromise of critical information" or "targeted scanning of networks" appear vague and do not strictly set the level of impact of an incident. The very act of ransomware does not find a place in the Rules and it left up to be inferred from such attacks if it falls into any of the various types specified.

[7] Nidhi Singal, 'Increasing cyber-attacks show why stringent cyber-security laws are need of the hour' (*Business Today*, 10 January 2021) <https://www.businesstoday.in/technology/news/increasing-cyber-attacks-show-why-stringent-cyber-security-laws-are-need-of-the-hour/story/427509.html>

[8] KV Kurmanath, 'Cyber-attacks: 66% of Indian organizations paid ransom to retrieve data access' (*The Hindu Business Line*, 24 June 2021) <https://www.thehindubusinessline.com/news/cyber-attacks-66-of-indian-organisations-said-they-paid-ransom-to-retrieve-data-access/article31907641.ece>

[9] 'The State of Ransomware 2021' (*Sophos*, April 2021) <https://secure2.sophos.com/en-us/medialibrary/pdfs/whitepaper/sophos-state-of-ransomware-2021-wp.pd>

[10] The Information Technology (The Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rule 2013, rule 5

Secondly, when it comes to reporting of an incident, the Rules state that the incident must be reported "within a reasonable time of occurrence or noticing the incident".[11] This statement leaves a lot open to interpretation by not fixing a time for reporting an incident. It also appears that reporting of an incident is not triggered if an attack takes place by a perpetrator or system located outside India but breaches the data of Indian consumers. It further remains silent on reporting of the incident to the data principal/the consumer.

Finally, CERT-In performs some key tasks such as conducting preventive testing and security audits as well as responding to incidents and conducting forensic analysis.[12] And yet the resources and infrastructure available to the agency is woefully inadequate. As per its last annual report in 2019, it had appointed only 90 technical IT security auditors.[13] Far less than required to manage the technical infrastructure of the country.

These inefficiencies and ambiguities result in a lot of unreported incidents. Concealment of data breaches seem to be the biggest hurdle. A lot of these inefficiencies are slated to improve with the arrival of the Personal Data Protection Bill (PDP) 2019. Under the Bill, a data fiduciary is required to report any personal data breach to the Data Protection Authority in the event the breach is likely to cause harm to a data principal[14]. A "personal data breach" under the PDP Bill means "*any unauthorized or accidental disclosure of, acquisition of, sharing of, use of, alteration of, destruction of, loss of access to, personal data that compromises the confidentiality, integrity or availability of personal data to a data principal*".[15] The word 'likely' under Section 25 indicates that the data fiduciary does not need to be completely certain that the breach would harm one or more data principals. The risk of harm is significant enough. However, interpretation of the term could lead to confusion. It would be necessary to establish the likely and necessary harm that a data principal would have to suffer such as those outlined under Recital 85 of the General Data Protection Regulation (GDPR). A quick response time period would also need to be established such as the GDPR which mandates a maximum of 72 hours delay in reporting a breach after becoming aware of it.[16] The necessary steps that should be taken to mitigate the risk with regards to the severity of the attack should also be stated. The Draft Bill enforces high penalties in the event a Data Fiduciary

[11] The Information Technology (The Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rule 2013, rule 12(1)(a)

[12]The Information Technology (The Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rule 2013, rule 9

[13] CERT-In Annual Report 2019 <https://www.cert-in.org.in/>

[14] The Personal Data Protection Bill 2019, sec 25

[15] The Personal Data Protection Bill 2019, sec 3(29)

[16] The General Data Protection Regulation (EU) 2016/679, art 33

fails to report a breach to the tune of "Rs. 50,000,000 or 2% of its total worldwide turnover of the preceding financial year, whichever is higher."[17]

When it comes to reporting an incident to the data principal, the Bill states that, a decision shall be made by the Authority whether the data fiduciary should notify the data principal of the breach, taking into account the degree of the harm that may be caused to the data principal, or whether the data principal must take action to mitigate the harm.[18] The Authority may order the data fiduciary to post information about the personal data breach on its website. The Authority may also publish information about the breach of data concerning the fiduciary on its own website.[19] There is no direct reporting to the data principal as under Article 34 of the GDPR.

Section 24 dictates that necessary safeguards and encryption must be complied with and to show that such safeguards were in place despite a cyber-attack to avoid any form of legal sanctions. The Data Protection Authority would have to decide whether such safeguards satisfy the requirements or not. If the Authority does not find the necessary safeguards satisfactory, it will invite additional sanctions of "Rs. 150,000,000 or 4% of its total worldwide turnover of the preceding financial year, whichever is higher."[20] A close look at both the PDP Bill and GDPR display that with regard to reporting and mitigating cyber incidents the PDP Bill has taken a leaf out of the GDPR's book. However certain aspects need to be clearly defined to avoid any ambiguity and create a better approach to safeguarding against cyber-attacks.

Further, India still grossly lacks from a pro-active approach by law enforcement agencies and authorities to bring down these menacing players. Ransomware hackers making use of disruptive technologies such as blockchain and cryptocurrencies do not make it any easier in the face of a global threat. It is about time the Rules from seven years ago are updated to cater to present times and remove the ambiguities in the present in the current version. Better infrastructure and resources for the agencies will certainly improve their efficiency and given the changing trends across the globe with a more attacking approach to tackling cyber incidents, it may be the right time to bring in amendments to give more teeth to CERT-In by giving it the power to investigate cybercrimes by itself or assist the relevant law enforcement authorities in investigations. They should also continue to expand cooperation from agencies across borders to facilitate a better response

[17] The Personal Data Protection Bill 2019, sec 57(1)
[18] The Personal Data Protection Bill 2019, sec 25 (5)
[19] The Personal Data Protection Bill 2019, sec 25 (6)
[20] The Personal Data Protection Bill 2019, sec 57(2)

to international threats, despite the fact that multiple MOUs have already been inked in favour streamlining resources and pooling of information.[21]

4. Conclusion

As a concluding note, a suggestion would be not to pay ransomware hackers. It is a fairly big gamble with a hope that the decryption tool would work in time or that there is a chance to retrieve back the ransom in full or even partially. The best alternative would be to invest in strong cyber security safeguards and comply with all the rules and regulation applicable under law to mitigate any kind of risk that occurs. India must move ahead with a two-pronged approach. Firstly, a targeted approach by agencies and authorities to weed out these cyber criminals by conducting full-fledged investigations pro-actively and secondly a clear well-defined mechanism to protect the sensitive data of individuals and mitigate risks in the event of a breach. A strong cybersecurity framework and even stronger awareness as to how these attacks take place will go a long way in preventing attacks in the future. Cyber-attacks such as ransomware are only going to grow in scale and sophistication and hence vigilance is the need of the hour and as it has been said time and time again. Prevention is the best cure.

[21] Yuthika Bhargava, 'CERT-In signs cyber security pacts with 3 nations' (*The Hindu*, 23 September 2016) <https://www.thehindu.com/business/Industry/CERT-In-signs-cyber-security-pacts-with-3-nations/article14022814.ece>