Globethics Repository



Stealing data : how to react to cyber criminal claims of extortion of moneys? : legal and ethical answers

This page was generated automatically upon download from the Globethics Repository. More information on Globethics see https://www.globethics.net. Data and content policy of Globethics Repository see https://repository.globethics.net/pages/policy.

Item Type	Book chapter
Authors	DUGGAL, PAVAN
DOI	10.58863/20.500.12424/4276063
Publisher	Globethics Publications
Rights	Globethics Publications;Attribution-NonCommercial-NoDerivatives 4.0 International
Download date	2026-11-07 16:02:11
Item License	http://creativecommons.org/licenses/by-nc-nd/4.0/
Link to Item	http://hdl.handle.net/20.500.12424/4276063

31

STEALING DATA: HOW TO REACT TO CYBER CRIMINAL CLAIMS OF EXTORTION OF MONEYS? LEGAL AND ETHICAL ANSWERS

Pavan Duggal, India[417]

Today data is the new oil of the data economy. Everywhere around us, we see data. This data has become the ubiquitous currency of our times and all this has happened, thanks to one big event that has happened during our lifetimes – the internet.

---

[417] 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. He is also Member of the International Board of Foundation of Globethics. Contact: pavan@pavanduggal.com. www.pavanduggal.com. © Globethics Publications, 2023 | DOI: 10.58863/20.500. 12424/4276063 | CC BY-NC-ND 4.0 International.

The internet is the second most significant event in human history after the advent of fire. No other event had such a massive and profound influence on the way how humans think, believe, perceive and do commerce.

With increasing adoption of the internet and with more and more people coming on to the internet bandwagon, data has become the new currency. Everybody is interested in not just receiving data but also generating data and transmitting data. No wonder, we have to realize that internet as a paradigm has transformed all of us from human beings into digital data entities.

We have all become global authors, global publishers and global transmitters of data. We are constantly producing data on a 24/7 basis, apart from constantly consuming data. Hence, data becomes very important. With the increased adoption of technology and new tech devices, almost everyone is saving their data in the digital format.

A majority of data is stored on devices while increasing quantum of data are now being stored on the cloud. From the perspective of corporates, this data becomes the crucial business resource as this business resource is huge not just for fulfilling and performing the day-to-day functions in the companies but also for the purposes of analysing past performances and predicting future trends, apart from being the raw material for reviews and analysis.

No wonder, data has become more crucial to legal entities than anything else. Today money is important, but I think with the passage of time, data will be far more important than money. This is because this data becomes capable of being monetized and once it is monetized, it can be used at any point of time by any stakeholder.

No wonder, data has become the most fertile target for potential attacks. Everybody wants to have access to not just to their own data but also the data of others. More and more cyber criminals want to have access to others' data so that the said data can then be used, monetized, disseminated as well as misused and abused.

This growing reliance on data has to be seen in the historical context of the times that we live in. At the time of writing this article, we are coming out of Covid-19 period. Covid-19 has not been just the public health emergency or the pandemic but it is also a cyber pandemic. The coming of Covid-19 has triggered irreversible changes, which are going to completely change the way how people interact in the online ecosystem.

In my book *New Cyber World Order Post Covid-19*[418], I have argued that by the time nations of the world are completely victorious against Covid-19, its current and subsequent waves of infections, the world will enter into a new cyber age, where the New Cyber World Order is awaiting us.

In this New Cyber World Order, states are going to become very powerful. But more significantly, cybercrime will become the new default normal. Also increasing cyber security breaches will be our constant companion.

Once we analyse both these trends of increasing cybercrimes and cyber security breaches, we quickly realize that the ultimate objective of both these paradigm shifts is primarily to target data. It is data which is targeted unauthorised, illegally or without permission and consent of the concerned data holder, so that this very data can then be used, monetized or abused in a variety of manners.

Today, we need to realize that we have already stepped into the data economy age. This is the economy which is dependent on the data, where data becomes the new currency of the new data economy. In this data economy, thus data assumes far more relevance. This becomes even more apparent when one looks at the various facts and figures pertaining to the growing quantums of data.

There were 79 zettabytes of data generated worldwide in 2021. By 2025, more than 150 zettabytes of big data will need analysis. The

[418] Duggal, P. 2020. New Cyber World Order Post Covid-19. Independently published, 53p.

COVID-19 pandemic increased the rate of data breaches by more than 400%. By 2027, the use of big data application database solutions and analytics is predicted to grow to $12 billion. [419] 463 ZB of data will be created every day by 2025. (Raconteur, 2020)[420]

A perusal of the aforesaid figures thus clearly tells us that the data bucket is constantly growing which is also a growing big triggering factor for growing cyber security breaches in the data economy age.

Today cyber security is being breached for a variety of purposes. But ultimately the focus of cyber security breach is to target, unauthorised access data and have unauthorized copies of data.

Cyber security breaches are happening all over the internet. State and non-state actors are both targeting and are being targeted by growing cyber security breaches.

During the third quarter of 2022, approximately 15 million data records were exposed worldwide through data breaches. This figure had increased by 37 percent compared to the previous quarter.[421] Between March 2021 and March 2022, the average cost of a data breach in the healthcare sector amounted to over 10 million U.S. dollars, up from 9.23 U.S. dollars between May 2020 and March 2021.[422]

It has been estimated that Ransomware accounts for nearly 24 percent of incidents in which malware is used (Verizon)[423]. By stealing 10

---

[419] Djuraskovic, Ogi. 2022. Big Data Statistics 2023: How Much Data is in The World? https://firstsiteguide.com/big-data-stats/

[420] 53 Important Statistics About How Much Data Is Created Every Day, FinancesOnline, https://financesonline.com/how-much-data-is-created-every-day/

[421] Petrosyan, Ani. Number of data records exposed worldwide from 1st quarter 2020 to 3rd quarter 2022, Statista, https://www.statista.com/statistics/1307426/number-of-data-breaches-worldwide/

[422] Petrosyan, Ani. Average cost of a data breach worldwide from May 2020 to March 2022, by industry, Statista, https://www.statista.com/statistics/387861/cost-data-breach-by-industry/

[423] 2019 Data Breach Investigations Report, Verizon, https://enterprise.verizon.com/resources/executivebriefs/2019-dbir-executive-brief.pdf

credit cards per website, cybercriminals earn up to $2.2 million through form jacking attacks (Symantec)[424]. The average total cost of a data breach was more than $1 million higher when working remote was a factor in causing the breach, compared to breaches in which working remote was not a factor (IBM).[425]

In these breaches, data becomes the final fertile target of attack. Therefore, stealing of data becomes the rampant trend of today's times. Once data is stolen, whether it is personal data or non-personal data, the same can then be monetized not just on the superficial net but also on the darknet and therefore new innovative and ingenious approaches are being adopted for the purposes of stealing data.

One of the most significant advances in this regard is the advent, constant growth and consolidation of ransomware as a paradigm. Ransomware is the big headache of today's times. But what exactly is ransomware. Let's see how ransomware is defined by major thought leaders as detailed below:-

Ransomware is a type of malware that prevents or limits users from accessing their system, either by locking the system's screen or by locking the users' files until a ransom is paid. [426]

Ransomware is a type of malicious software (malware)[427] that threatens to publish or blocks access to data or a computer system, usually by encrypting it, until the victim pays a ransom fee to the attacker.[428]

---

[424] Internet Security Threat Report, Executive Summary, 2019, ISTR 24, https://docs.broadcom.com/docs/istr-24-executive-summary-en

[425] IBM. 2022. Reports. Cost of a data breach 2022, https://www.ibm.com/reports/data-breach.

[426] Ransomware, Trend Micro Incorporated, https://www.trendmicro.com/vinfo/us/security/definition/ransomware#:~:text=Ransomware%20is%20a%20type%20of,until%20a%20ransom%20is%20paid.

[427]What Is Malware? Proofpoint, https://www.proofpoint.com/us/threat-reference/malware

[428] What Is Ransomware? Proofpoint, https://www.proofpoint.com/us/threat-reference/ransomware

Ransomware is a type of cyber extortion where a malicious actor infiltrates an environment and encrypts and exfiltrates files, denying access and threating disclosure, unless the victim pays a ransom.[429]

Ransomware is a specific type of malware[430] that extorts victims for financial gain. Once activated, ransomware prevents victims from interacting with their files, applications or systems until a ransom is paid, usually in the form of an untraceable cryptocurrency like Bitcoin. In some cases, the victim is instructed to pay the perpetrator by a set time or risk losing access forever. In other cases, the perpetrator intermittently raises the ransom demands until the victim pays.[431]

Ransomware began with small beginning.

The first documented ransomware, *AIDS Trojan or PC Cyborg*, was delivered at the World Health Organization's AIDS conference in 1989 using floppy disks, demanding a payment to be sent to a postal office box in Panama. This malicious code was not encrypting the files content as we know it today, but the filenames only. It was however enough to take down the systems and cause disruption. [432]

Today ransomware has various salient features. Ransomware has become so severe today that it has becoming to become the default cyber security challenge and headache of today's times. This becomes further evident when one looks at various facts and figures of ransomware.

Ransomware cost the world $20 billion in 2021. That number is expected to rise to $265 billion by 2031. Recovering from a ransomware attack cost businesses $1.85 million on average in 2021.Out of all ran-

---

[429] Ransomware, Gartner Glossary, https://www.gartner.com/en/information-technology/glossary/ransomware

[430] What Is Malware?, Proofpoint, op. cit.

[431] Ransomware, Cyberark Glossary, https://www.cyberark.com/what-is/ransomware/

[432] Lessing, Marlese. 2020. Case Study: AIDS Trojan Ransomware, https://www.sdxcentral.com/security/definitions/what-is-ransomware/case-study-aids-trojan-ransomware/

somware victims, 32 percent pay the ransom, but they only get 65 percent of their data back.[433]

There was an 85% increase in ransomware attacks since 2020. (Palo Alto Networks, 2021). Reports expect there to be a ransomware attack every two seconds in 2022. (Cybersecurity Ventures, 2022) [434]

The aforesaid figures tell us that every stakeholder today has to be prepared for ransomware. It is not only a question of "if", but it is only a question of "when" you would become a victim of ransomware attack.

Once a ransomware attack takes place, the encryption algorithms come in and encrypt entire data and therefore money is sought for the purposes of providing the key for decrypting the said encrypted data.

That claim for money is often the cherry on the cake. This claim of money is made in the form of crypto-assets and Bitcoins so that they can become less traceable and the chances of law enforcement agencies reaching the ultimate cyber criminal gets further diminished.

Whatever kinds of ransomware attacks can take place, whether it is simplicitor ransomware attacks or wiper malware attacks, ultimately seeking moneys becomes the primary objective. Huge quantum of moneys have been asked on ransomware attacks across the world.

On November 8, 2021, a ransomware attack took place against *MediaMarkt*, Europe's largest electronics retailer. The Hive gang[435], which carried out the attack, initially demanded a ransom of 250 million USD, but the amount was reduced to 50 million USD after a while.[436]

---

[433] Kochovski, Aleksandar. Ransomware Statistics, Trends and Facts for 2023 and Beyond, https://www.cloudwards.net/ransomware-statistics/

[434] Stouffer, Clare. 2022. Ransomware statistics: 102 facts and trends you need to know in 2023, Norton, https://us.norton.com/blog/emerging-threats/ransomware-statistics#

[435] Dark Web Profile: Hive Ransomware Group. 2023. SOCRadar Research, https://socradar.io/dark-web-profile-hive-ransomware-group/

[436] 20 Interesting Facts About Ransomware, SOCRadar, https://socradar.io/20-interesting-facts-about-ransomware/

The highest-profile attack of 2021 was arguably the one on Colonial Pipeline. This provided over 40% of the East Coast's fuel, but as the ransomware attack left the company unable to bill properly, it was forced to suspend operations temporarily. Even though the company paid a $4.4 million ransom, it took a long time to get everything back online, leading to fuel purchasing restrictions in 17 US states. [437]

Ransomware group DarkSide targeted the chemical distribution company Brenntag and demanded a payout of $7.5 million in Bitcoin. (Brenntag, 2021)

The hacker group behind an oil company attack allegedly acquired $90 million in ransom payments in only nine months from around 47 victims. (Fox Business, 2021)[438]

Garmin, a major player in the tech space, suffered a severe breach that brought its GPS services offline for several days. In order to regain control, the company allegedly paid a $10 million ransom.

The US Treasury has linked more than $5 billion of Bitcoin transactions to ransomware.

The highest ransom demanded from a victim reached $70 million in 2021 (Blackblaze, 2021)[439]

Easily it is apparent this entire paradigm of ransomware throws up large number of crucial ethical and legal questions. Is it ethical to steal data? The answer for that is crystal clear no. Is it ethical to engage in ransomware? The answer is the same, also no. Is it ethical to ask for

---

[437] Cook, Sam. 2022. 2018-2022 Ransomware statistics and facts, Comparitech, https://www.comparitech.com/antivirus/ransomware-statistics/

[438] Brooke Crothers. 2021. JBS ransomware attack points to ominous trend targeting critical industries by foreign actors, FOXBusiness, https://www.foxbusiness.com/technology/jbs-ransomware-attack-trend-targeting-critical-industries-foreign-actors

[439] Clancy, Molly. 2021. The True Cost of Ransomware, Backblaze, https://www.backblaze.com/blog/the-true-cost-of-ransomware/; Ransomware statistics: 102 facts and trends you need to know in 2023, Norton, https://us.norton.com/blog/emerging-threats/ransomware-statistics#

cyber criminal claims for extortion of moneys? The answer here is also crystal clear, an emphatic no.

The answers to all the three questions from a legal standpoint are also a crystal clear no. This is so because data ethics as an emerging science has been evolving which has stipulated various principles pertaining to ethical use of data. Hence, the ethical expectation of every data stakeholder is that their data is going to be ethically used and are not unauthorised or unethically accessed, downloaded, copied, extracted, modified, deleted or prejudicially impacted in any manner whatsoever.

Since it is unethical to engage in ransomware, it is a logically corollary that it is unethical to make payments for cybercriminal claims of extortion of moneys. This is so because the said conduct is neither ethical, nor prudent.

Further, once you start paying money to cyber criminals in a ransomware attack, you effectively give a confirmation to the fact that you are not just the fertile target, as you have the capacity to pay, but also that you can tomorrow become a repeat target of such kinds of cybercriminal claims of extortion of moneys.

That is the reason one finds that law enforcement agencies across the world are encouraging people not to make extortion payments to cyber criminals.

Evidence in this regard is well established. The Federal Bureau of Investigations in the United States has gone ahead and evolved its thought process.

Below is an advisory taken directly from the U.S. FBI

"The FBI does not advocate paying a ransom, in part because it does not guarantee an organization will regain access to its data. In some cases, victims who paid a ransom were never provided with decryption keys. In addition, due to flaws in the encryption algorithms of certain malware variants, victims may not be able to recover some or all of their data even with a valid decryption key.

Paying ransoms emboldens criminals to target other organizations and provides an alluring and lucrative enterprise to other criminals." [440]

Apart from the aforesaid, various other statutory authorities in different parts of the world have also been encouraging people not to make extortion payments.

Such an approach is logical and ethical apart from legal as well and such an approach is also backed by emerging principles of data ethics as a science. The said ethical principles are also now being enshrined in legal instruments. For example, in the US, the new legal framework has been passed which has actually made the making of payments to ransomware attacks as a criminal offence.

US law frameworks now stipulate that any person, who makes payment to ransomware attack has to mandatorily disclose the same to the law enforcement agencies, thus exposing the said person to legal consequences.

Victims who pay ransoms might also be subject to criminal or civil penalties in some cases—for example, where a ransom payment is made knowingly to an entity either designated as a foreign terrorist organization or subject to sanctions by the Department of the Treasury. Nevertheless, policy considerations, mitigating factors, and prosecutorial discretion may weigh against enforcement in such instances.[441]

One of the biggest problems across the world is that most of the countries don't yet have dedicated legal frameworks on ransomware to deal with the cyber criminals claims of extortion of moneys. Most countries have in place national penal laws which make extortion an offence.

However, when one talks about cyber criminal extortion of moneys, it is clearly a manifestation of extortion of moneys and hence can be

---

[440] Organizations across the globe need to develop a ransomware payment policy, anticipating a potential future attack, EY Global, https://www.ey.com/engl/consulting/ransomware-to-pay-or-not-to-pay

[441] Ransomware and Federal Law: Cybercrime and Cybersecurity, Congressional Research Service, 2021, https://crsreports.congress.gov/product/pdf/R/R46932

covered under the traditional penal laws. Nevertheless, many countries are now increasingly looking to devise new laws pertaining to ransomware.

As of now, most of the countries don't have dedicated laws on ransomware. Similarly, most of the countries don't have laws on payment of moneys demanded in ransomware or payment of cyber-criminal claims of extortion of moneys.

This is a very fertile time in today's times as the ethical and legal principles will need to go hand-in-hand while crystalizing a legal response to cyber criminality. Ethical and legal principles will have to find appropriate mention in the respective national legal frameworks, which are now developing to counter the cyber criminal claims of extortion of moneys and the growing ransomware demands for moneys.

There is a need for ethical principles concerning data ethics to be incorporated in the forthcoming new legal frameworks on ransomware, that are now being discussed and deliberated in different parts of the world. Further, ethical principles need to be inculcated as an integral part of the new emerging legislative approaches, that are developing in countries to deal with the challenges of emerging technologies and their appropriate regulation.

Similarly, when Artificial Intelligence (AI) is used for the purposes of facilitating cyber criminal claims of extortion of moneys, those elements will also have to be appropriately addressed by ethical and legal principles put together.

It will be ethical for lawmakers to not just mandate such kind of activity as unethical and illegal but more significantly also to stipulate appropriate responsibilities and liabilities for the relevant Artificial Intelligence ecosystem stakeholders in the event AI is misused for cyber criminality.

Thus moving forward, some essential weapons will have to be part of everybody's arsenal in fighting the menace of cyber criminal claims of extortion of moneys in the context of stealing of data.

Cyber resilience will have to play a very important role in this regard. Cyber resilience is a new concept and is slowly gaining more currency. It has been defined by varius stakeholders in different ways.

Cyber resilience is the ability of an organization to enable business acceleration (enterprise resiliency) by preparing for, responding to, and recovering from cyber threats.[442]

Cyber resilience is the ability of an organisation to protect itself from, detect, respond to and recover from cyber attacks.[443]

Cyber resilience refers to an organization's ability to continue business operations despite a cybersecurity or data loss incident.[444] Cyber resilience is a measure of how well an enterprise can manage a cyberattack or data breach while continuing to operate its business effectively.[445]

Cyber resilience presumes that you will be under attack. The question is how can you avoid panic and quickly come back to a state of normalcy after getting attacked. This forms the foundational fulcrum of cyber resilience.

Further, cyber hygiene will have to play a very important role in this regard. Cyber hygiene has been defined by various stakeholders.

Cyber hygiene refers to the steps that users of computers and other devices can take to improve their online security and maintain system health. Cyber hygiene means adopting a security-centric mindset and

---

[442] What is Cyber resilience? Microfocus, https://www.microfocus.com/en-us/what-is/cyber-

[443] Cyber Resilience, IT Governance, https://www.itgovernance.co.uk/cyber-resilience

[444] Cyber resilience definition, Druva, https://www.druva.com/glossary/what-is-cyber-resilience/

[445] What is Cyber Resilience? Digital Guardian, https://digitalguardian.com/blog/what-cyber-resilience

habits that help individuals and organizations mitigate potential online breaches[446]

Cyber hygiene is a reference to the practices and steps that users of computers and other devices take to maintain system health and improve online security. These practices are often part of a routine to ensure the safety of identity and other details that could be stolen or corrupted. Much like physical hygiene, cyber hygiene is regularly conducted to ward off natural deterioration and common threats.[447]

Cyber hygiene is a set of habitual practices for ensuring the safe handling of critical data and for securing networks. It's like personal hygiene, where you develop a routine of small, distinct activities to prevent or mitigate health problems. Cyber hygiene practices include the inventory of all endpoints connected to a network, vulnerabilities management, and the patching of software and applications.[448]

The European Union's Agency for Network and Information Security (ENISA) states that "cyber hygiene should be viewed in the same manner as personal hygiene and, once properly integrated into an organization will be simple daily routines, good behaviors, and occasional checkups to make sure the organization's online health is in optimum condition".[449]

---

[446] Top Tips for Cyber Hygiene to Keep Yourself Safe Online, Kaspersky, https://www.kaspersky.com/resource-center/preemptive-safety/cyber-hygiene-habits

[447] Brook, Chris. 2022. What is Cyber Hygiene? A Definition of Cyber Hygiene, Benefits, Best Practices, and More, Digital Guardian Blog, https://digitalguardian.com/blog/what-cyber-hygiene-definition-cyber-hygiene-benefits-best-practices-and-more

[448] Null, Christopher. 2021. What Is Cyber Hygiene and Why Does It Matter?, Tanium Inc., Blog, https://www.tanium.com/blog/what-is-cyber-hygiene-and-why-does-it-matter/

[449] Tyas Tunggal, Abi. 2022. What is Cyber Hygiene and Why is it Important? Blog, UpGuard Inc., https://www.upguard.com/blog/cyber-hygiene

Therefore, cyber resilience and cyber hygiene will have to play important response mechanisms so as to prevent or minimize the impact of cyber criminal claims of extortion of moneys in the context of stealing of data.

Backups will have to become the number one default normal. Backups, backups, backups will have to be the only mantra going forward, as stakeholders would be required to back up their data every 2-3 days in order to ensure that their operations don't go offline in the event they are hit by ransomware attack and either unable or do not want to make payment for cyber criminal claims of extortion of moneys.

Backups represent an ethical, legal and pragmatic approach to the constant challenge of cyber criminal claims of extortion of moneys in the context of stealing data. A Backup basically means the process of taking copies of your data that has already been generated.

Backup copy means the copy of at least those source data (software assets and information assets) which are needed for the recovery and/or reestablishment of business processes.[450]

A backup is another resource used to make sure an activity can go on, or deploy an alternate project if a primary one cannot be done. Saving data on disc or offsite prevents important information from being lost, stolen, or sabotaged.[451]

Backing up data brings forward its own ethical and legal considerations. In today's times, when we all are being flooded by constant new volumes of data with each passing day, it would be so tedious and time consuming to try and reconstruct data. A backup is an ethical approach – since it is your data, it is your duty to have a copy. Once your data is duly backed up, at least it tends to give you a sense of peace of mind. Without this precaution, the entire data would be lost once and for all in the event of a ransomware attack or data wipe out.

---

[450] Lawinsider, Dictionary, https://www.lawinsider.com/dictionary/backup-copy

[451] Ibid, https://thelawdictionary.org/backup/

The time has come for us to revise our thinking and find new approaches to deal with the challenges of data theft and the cyber criminal claims of extortion of moneys. We will have to become more proactive, more fast and flexible in our thought process. We will have to take it as a given that yes, we will be hacked and our data is going to be constantly attacked and breached. Hence, any kind of data breach of data stakeholders should not take us by surprise. Hence, we will need to constantly rely upon not just new volumes of data but also preserving and retaining properly the old data that is generated. Because in a data driven world, it is only data that is going to be our biggest source of empowerment and source of protection. This becomes even more important when one looks at the facts and figures pertaining to growing data theft and projected trends in this regard.

- The US suffers from the most data breaches
- The biggest data breaches in 2021 were:
- Comcast (1.5 billion)
- Brazilian resident data leak (660 million)
- Facebook (533 million)
- LinkedIn (500 million)
- Byeka (400 million)

According to the Symantec Security Summary, April 2021, ransomware payments jumped 171% in 2020, with the highest payout doubling to $10 million.[452]

From the perusal of the aforesaid facts and figures, it thus becomes very clear that it is ethical not just to produce and deal with your own data but also that you take appropriate steps to protect data. Since your data could potentially become a target of potential theft, it becomes

[452] O'Driscoll, Aimee, 2023. 30+ data breach statistics and facts, Comparistech Inc., Blog post, https://www.comparitech.com/blog/vpn-privacy/data-breach-statistics-facts/

absolutely imperative that all ethical and legal, pragmatic and practical steps must be taken so as to protect your data.

If appropriate methodologies of cyber hygiene, cyber resilience and backups are adopted, then the potential losses caused by data theft and the consequent cyber criminal claims of extortion of moneys could be potentially minimized to the best lowest extent possible.

However, the world is walking in a complete different new direction. Every 11 seconds, a company became victim of ransomware attack in 2022. It is expected that by the end of 2023, in every 9 seconds, a company is likely to become a victim of ransomware attack. Recovering from ransomware attacks today are on average very costly for for legal entities.

Hence, it is a given fact that ransomware attacks will keep on increasing. Data theft will constantly grow and the cyber criminal claims of extortion of moneys would also multiply with each passing day, month and year. The absence of any international legal frameworks to control or deal with such kinds of data theft or ransomware attacks or cyber criminal claims of extortion of moneys further complicates the entire scenario.

Since data theft happens on the internet which is a transnational paradigm, it also assumes extra-territorial nuances. Further, as the internet has made geography history, it is possible for a legal entity or person to sit in one jurisdiction and steal data located in another jurisdiction and also ask for cyber criminal claims of extortion of moneys from stakeholders in a third jurisdiction.

Hence, this entire issue of stealing data brings forward various complicated issues of internet jurisdiction and connected nuances. The new trends are clearly telling us that the only way to protect yourself is to empower yourself and strengthen your cyber security. Cyber resilience and backups will have to be the only mantra going forward for the purposes of protecting yourself from becoming victim of untoward consequences because of loss of data.

To conclude, it can be said that in today's world, data ethical principles, exist but they have not been given the right kind of importance, thrust or impetus. Instead, cyber criminals are going ahead and acting with impunity to steal people's data and thereafter use it for extortion.

These entire paradigms of stealing of data for cyber criminal claims of extortion of moneys need to be handled, both from legal and ethical standpoint. The ethical principles concerning data theft, which are evolving in data ethics as a discipline, need to be specifically incorporated by legal frameworks which have been formed so as to meet up with the challenges of ransomware, data theft and ensuing extortion.

A lot of work needs to be done now. Currently, it appears that the legal and ethical frameworks are lagging far behind as compared to the speed with which cyber criminals are moving ahead in terms of data theft. The onus will be on the cyber ecosystem stakeholders, specifically on lawmakers and governments to come up with effective and ethical principles incorporated in their national legal frameworks to deal with the menace of stealing of data, ransomware and raising of subsequent cyber criminal claims of extortion of moneys.

This is a very interesting space to watch as time passes by.