Page 2808 - 2821 **DOI:** *https://doij.org/10.10000/IJLMH.111673*

INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

Volume 4 | Issue 4

2021

Corporate Governance and Cyber Security

SIMRAN SINGH[1] AND VAISHNAVEE UPRETI[2]

ABSTRACT

The continuous rise in technology has been of great help to the business world but has also raised the risk of cyber breach. The rise in cyber breach from 2006 to the present day has increased from 3 million to 540 million in Facebook alone. They used to be individuals but now they are organizations which professionally work for anyone who hires them to extract data. The risk and gravity of this breach is not realized by people until it happens with them. Privacy and data management have become the core issues of corporate governance in India. A 2019 Chief information Officer (CIO) survey by Force point and Frost & Sullivan found that 69% of Indian organizations are at a risk of data breach. It also found that not enough C-level teams are involved in cyber security preparations, with only 34%, mainly BFSI (Banking, Financial Services and Insurance), telecom and IT & BPO companies involved in it.

I. INTRODUCTION

India has been growing digitally and with this technological development there has been a change in the way businesses are being done, there has been a development in the interconnected business activities. It is due to these interconnected business activities that there has been an increase in digitization, which has brought with itself privacy and data security risks. Data privacy means the ability of organizations or individuals to determine how much information can be shared with third parties in a safe manner. The determination of how information can be protected from cyber-attacks, unapproved access, etc. is done through a mechanism called cybersecurity.

There are a ton of interesting points with regards to information security. Most organizations depend on cloud-based platforms wherein they'll simply need to confide in what the platform needs to state about how they're encrypting and protecting data. Some of the government led organizations and research centers have their own servers to manage data which isn't even connected to any external network to worry about protection. But mostly, cloud platforms and online services have taken over which may or may not be a good thing depending on how the

[1] Author is a Lawyer in India.
[2] Author is a Lawyer in India.

 [ISSN 2581-5369]

big players choose to use that data.

Unlike Cambridge Analytica, not a lot of companies have the infrastructure to break into Facebook or Google's algorithms to discover what precisely they're doing with the information contingent upon the security of these frameworks, even a common man can break into someone's database and take information as long as it's on the internet (most of which is). It's only as secure as the amount of money you spend on safety and encryption. In any case, on the other hand, regardless of how secure a framework is, there's always a possibility that a better-equipped hacker is able to crack the code.

II. PRIVACY RISKS IN CORPORATE GOVERNANCE

With the technological advancement there has also been an increase in cyber risks by organizations being more prone to cyber attacks, with the cyber attacks comes the risk of data breaches. the data breaches have been multiplying in the corporate world due to which addressing the cybersecurity issues becomes all the more important. Extradition of personal data from companies by hackers is one of the main issues faced by organizations and can be looked after only through strict corporate governance in the matters of data protection. Earlier only developed nations had been a target of cyber-attacks but recently Indian companies too have been on par with the other nations with respect to cyberattacks. A report by the National Crime Records Bureau (NCRB), Ministry of Home Affairs, Government of India, shows a 78% increase in cases reported under the Information Technology (IT) Act in 2019 from the year 2014. The number of cases recorded increased from 9,622 in 2014 to 44,546 in 2019[3].

Cybersecurity has become a governance issue because there might be a lack of expertise in the board members to deal with and to understand the complexities of cybersecurity. Though the board of directors need not be directly involved in the efforts to prevent the happening of cyberattacks but they can set up a committee of technical experts which can overlook all the matters within their expertise. Cyber breaches can result in legal liabilities for corporations which makes it very clear that cybersecurity has become a part of corporate governance.

Various types of privacy risks involved in corporate governance

A recent report by Kearney suggests that cybersecurity has been a key issue amongst almost every organization and that cyber-attacks have been at the top of the list of business risk for three consecutive years[4]. The kinds of privacy threats and risks are very vast in number and do

[3] Ministry of Home Affairs, Government of India, Crime in India, National Crime Records Bureau (2015-2019).
[4] Rising to the challenge, Kearney (Apr. 22, 2020, 5:30 PM), https://www.kearney.com/web/global-business-policy-council/article?/a/rising-to-the-challenge_2018.

not fail in keeping up with the technological changes.

An attempt has been made to discuss a few types of privacy risks that organizations face.

1. Malware – it is a form of cyber-attack in which a malicious software is introduced or installed in the system disguised as a legitimate software which gives unauthorized access to the system, without the user having a knowledge of the same. This malicious software can be introduced through various mediums like email attachments, software downloads, etc.
2. Ransomware – this is a type of malware which, when opened locks up the system of the user by encrypting it so that it is inaccessible and can be unlocked only once a hefty ransom is paid to the attacker. This is the most advanced and dangerous kind of cyberattack.
3. Phishing – under this type of attack a fake web page or email which looks like it is from an authentic source is created and the user is manipulated to click on that link. The aim of it is to extract personal information and sensitive data.
4. DDoS – Under Distributed Denial of Service (DDoS) attacks the system gets overloaded with requests to access the server and ultimately resulting in the server being crashed.
5. Internet of Things – Due to the reliance of companies on IoT applications their data has become more vulnerable to attacks.
6. Password stealing pr password attacks – this involves a cybercriminal trying to gain access to a network by programming to hack the current password. This is the reason it is vital to not use the same password across the board and to keep changing the login details every once in a while.
7. Drive-by downloads and malvertising – drive-by downloads a malicious software is installed when the victim visits a webpage. Malvertising is when the victim clicks on a malicious advertisement.
8. Cybersquatting – the attacker tries selling the domain name of the victim to the victim's competitors or anyone else.

Factors which lead to privacy risks and cause cyber breaches

There are various factors and links which can result in organizations being prone to data or privacy breaches and can lead to the increase in number cyberattacks. An attempt has been made to discuss a few of the factors:

 [ISSN 2581-5369]

- Insider threat – this can said to be the top most factor for organizations being prone to cyberattacks. Insiders mean the people working in the organization like employees, business partners etc., who have access to security systems. This also includes the employees falling a prey for phishing emails, clicking on malicious links etc., and employess misusing their privilege to access security systems. As per the a survey conducted by PwC, an insider caused nearly 15 security incidents for every 10 incidents Insider threats tackled at multiple levels 15 incidents caused by insiders for every 10 incidents caused by an outsider caused by an outsider in 2015; yet, a majority of businesses are unprepared for insider threats[5].
- Passwords – it should be made sure that all the business accounts have been secured with a password and the employees should be strictly asked to not share their passwords with anyone.
- Software - another factor responsible to privacy threats can be not updating the software regularly, due to which it can easy for the hackers to get access to the system.
- Other organizations – if the organization with which one is dealing does not have stringent cyber security policies then it makes the other organization too with which it is dealing prone to cyberattacks and attackers can easily gain access and enter the system. A conversation about the cybersecurity policies with potential vendors is suggested, in order to curb the privacy risks.
- BYOD Practice – Bring Your Own Device (BYOD) is a practice in which the employees can bring their own devices to work on and many organizations have been following this. The employers forget to consider the security risks such a practice brings with itself. A good and strong BYOD policy can be framed and it can be ensured that all employees strictly adhere to it.
- Lack of awareness about potential cyber risks that can take place and lack of interests from the employees in knowing about the same.
- Lack of cybersecurity policy and lack of a recovery plan – the companies not prioritizing the framing of cyber security policies and not getting their employees to know about the same is too risky at such a stage of technological advancement. In case of an attack it is a must or any organization to have a recovery plan in place in order to

[5] Turnaround and transformation in cyber security: India update, Pricewaterhouse and Coopers, 10 (2015).

 [ISSN 2581-5369]

minimize the damages caused but due to lack of knowledge and interest there are very few organizations that have taken this seriously.

Few principles and guidelines that can be adopted by the organizations

- Cover cybersecurity basics to not be more vulnerable to attacks as cyber criminals require very few vulnerabilities to get access to sensitive contents.
- Failing to understand what exactky generates corporate cybersecurity risks.
- Coming up with a cybersecurity policy and sensitizing everyone in the organization about the same while also sticking to those policies.
- Knowing the organizaion's data and how it is used and maintained. This simply does not mean assigning the work to the Human Resource manager or IT but the data must also be audited on a regular basis.
- Having a recovery plan to be prepared for the worst.
- There must be predictive analytics done by machine learning that help in identifying how the cyber-attack looks like, when the cyber-attack might occur, what is its source and how can it be counter attacked. All these are very well known to IT personnel and is extremely useful for DDoS attacks.
- Having data back-up plan to get the services and systems back online with minimal downtime which can result in data losses.
- While dealing with other organizations the relationship must be based on Service Level Agreements (SLAs) to ensure that there are no potential risks of data exposure and even if there are such an agreement provides legal assurance in case of any cyber-attack or data breach through that company or third party that is being dealt with.
- Purchasing cyber security insurance. With the increasing cyber crimes many organisations have been investing in cyber security insurance so that in case of a cyber-atttack either on their own systems or of their suppliers and partners the companies are protected financially.

There are certain measures which can be adopted by the white hat hackers (ethical hackers) in helping organizations to counter attack on the source, which is always by black hat hackers (unethical hackers), that is initiating an attack, provided these methods do not bring any liability under the laws dealing with cyber offences.

 [ISSN 2581-5369]

- Beacons – these are subtly hosted graphics or programs that reveals the IP address of the source once a contact has been made with a remote server.
- Honeypots – these are digital honey traps which tricks the cyber attackers into taking an action against an artificial network thereby allowing the white hat hackers of the organization to access and gain control and thereby counter attack the source, without causing any damage to the real network and servers of the organization.
- Bug Bounties – these are bugs or programs that are used by the white hackers to know the errors or vulnerabilities of the system and also to identify the source of attack used by the black hat hackers.
- Sinkholes – these are method used to redirect the source of attack away from that of the organization's IP addresses and severs and are commonly used in DDoS attacks.

III. EXISTING LEGAL FRAMEWORK

In India though the cybersecurity in corporate governance is still at the beginning stage, there are various provisions in law which deal with cyber offences.

Indian Penal Code, 1860 –

In case of electronic theft, by breach of confidence by current or former employees Sections 379, 409, 419 and 420 of IPC which provides for punishment of theft, punishment of imprisonment and fine for criminal breach of trust by a public servant or an agent, punishment of cheating by personation and punishment of cheating respectively.

Copyright Act, 1957 –

In case of electronic theft section 63 of Copyright Act too is applicable which gives a punishment for infringement of copyright.

Information Technology Act, 2000 –

Section 43 of the Act provides that *"If any person accesses a computer, computer system or computer network without permission of the owner, or downloads, copies and extracts any data, or causes disruption of any system; inter alia, they will be liable to pay damages by way of compensation to the person so affected".* This section covers the punishment for unauthorized access, ransomware, malware and all the attacks of a similar nature. Section 43(f) of the Act gives punishment for DoS attacks (Denial of Service). Section 43A provides for an uncapped compensation which the corporate body will be liable to pay in case of failing in protecting any sensitive personal information or data in a system which it owns, controls or

 [ISSN 2581-5369]

operates. Sections 45 and 70B will be applicable when there is a failure to make reports or non-compliance with directions under the CERT-In Rules, 2013; which will be dealt with a little later. Section 65 of the Act provides punishment for concealment or destruction of computer source documents. Section 66 provides for the punishment of committing any act dishonestly or fraudulently that are referred to in section 43. Section 66B gives the punishment for receiving stolen computer resources or communication devices in a dishonest manner, but mere possession of such tools is not criminalized. Section 66C of the Act provides for punishment of using electronic signature, passwords or any other such unique identification feature of any other person in a dishonest or fraudulent manner. This can be used when there are phishing attacks on the server. Section 66D provides punishment for the person using any compute resource for cheating by impersonating someone. Section 66F specifically define cyberterrorism, which means ay crime which has the intention of threatening the unity, integrity, security or sovereignty of India or strikes terror amongst people or denies or causes denial of access to any person who is authorized to access any computer resource. This section also tells us what the specific conditions are which classify an offence as cyberterrorism. Section 72 provides for punishment for breach of confidentiality and privacy and section 72A provides the punishment for disclosing personal information about a person, without such person's consent or in breach of a lawful contract, knowing that it will cause harm. Section 74 provides the punishment for creating and publishing an electronic signature certificate for any unlawful or fraudulent purpose.

The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 (SPDI Rules) –

Under these rules apart from the information that is sought by governmental agencies the corporate bodies before the disclosure of information to any third party are first required to get the permission from such information providers and such companies are also required to have such an information security system that it protects those informational assets.

Information Technology (The Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rules, 2013 (CERT-In Rules) –

These rules require corporates as well as individuals to report any cybersecurity incidents that have taken place mandatorily to CERT-In in order to get assistance for the same. Non-compliance of the same may attract penalties under Sections 45 and 70B of the IT Act.

National Cybersecurity Policy, 2013 –

The aim of this policy is to create a secure cyberspace to strengthen the regulatory framework

 [ISSN 2581-5369]

for corporate bodies in order protect information and data. It also suggests and encourages organizations, both public and private, to assign one person in as the Chief Information Security Officer (CISO) in order to take all the necessary initiatives and efforts to strengthen the cybersecurity policy.

Companies (Management and Administration) Rules, 2014 (CMA Rules) –

It mandates companies to ensure that electronic records are secured, including protection against unauthorized access, tampering of servers, etc.

Uday Kotak Committee on Corporate Governance, 2017 –

This committee was constituted by SEBI in June 2017 and its aim was to improve the standards of corporate governance of listed companies in India. it was acknowledged by the committee that cybersecurity has become a priority in ensuring that the shareholder's interest is safeguarded.

Information Technology (Information Security Practices and Procedures for Protected System) Rules, 2018 –

These rules specify certain cybersecurity practices that an organization which has a protected system must follow, like designating a Chief Information Security Officer (CISO), maintaining regular backups, etc.

Application of these laws in certain cases –

In *Gagan Harsh Sharma and Others v. State of Maharashtra and Others*[6] the employee who was accused of stealing the software which was developed by his company had been punished under Sections 420, 408 and 379 of the IPC and the court did not allow an action which was brought under Section 66 of the IT Act as it would lead to double jeopardy.

In *State Bank of India v. Chander Kalani and Others*[7] there was an alleged hacking of the complainant's email id and a confidential information had been leaked with regard to the complainant's bank account. SBI was negligent in disclosing the detail's of the bank account of the complainant and has responded to fake emails, it was held that under Section 43A of the IT Act the bank was liable to pay the compensation to the complainant.

In *Umashankar Sivasubramanian v. ICICI Bank*[8] the complainant received a security email update from the bank and did not know about it being fake so entered all his bank account

[6] 2019 ALL MR (Cri) 595.
[7] Cyber Appeal No. 13 of 2015, M.A. No. 282 of 2017.
[8] Civil Petition No. 2462 of 2008.

 [ISSN 2581-5369]

details, after doing so he realized that certain amount had been deducted from his bank account. It was held that the bank failed in exercising due diligence by not preventing an unauthorized access as under Section 43 of the IT Act and was liable to pay the complainant the compensation for the same.

In *National Association of Software and Service companies v. Ajay Sood and Others*[9] the defendants were impersonating the plaintiffs and using their trademark "NASSCOM" to send fraudulent emails in order to obtain personal data. Through this case the concept of phishing was introduced in Indian law.

In *Raymond Limited v. Raymond Pharmaceutical Pvt. Ltd.*[10], the plaintiff seeked an injunction against the defendant for using the mark "Raymond" as their domain name. it was held that the defendant was not guilt either of cybersquatting or copyright infringement and said that the elements of cybersquatting wasn't satisfied by the defendant.

In a case of breach of confidentiality, the defendants had been refrained from misusing trade secrets and confidential information of the plaintiffs without their consent, the Delhi High Court had also ordered Google which was another defendant in the suit to block the email accounts of the other defendants in the suit[11].

IV. DATA PROTECTION: NEEDS THE BOARD'S ATTENTION

The role of directors of a company is to first and foremost execute efforts into properly perceiving, prioritizing and implementing the required changes in order to comply with data protection.

1. Cyber risk is an IT issue

The board shall be proactive in conducting internal audits to visualize its cybersecurity programs covering all domains. This may offer corporate leverage against external security organisations.

2. Cyber risks have crucial legal consequences

The risk related to the third-party service provider, where India happens to possess a significant task in outsourcing the board of directors must list of all third-party relationships and guarantee acceptable agreements are set up. Nations around the world have numerous legal regimes they follow, which makes the board susceptible to be aware of laws relating to privacy, security and

[9] 119 (2005) DLT 596.
[10] 2017 (69) PTC 79 (Bom.)
[11] *Olive e-business v. Kirti Dhanawat and Others,* Delhi High Court, CS(COMM) 610/2018.

breach.

3. **Cyber-risk needs to be the agenda of customary board conversation**

The board must have access to sufficient cybersecurity aptitude and need to commit time for conversations on this theme conjointly get internal cybersecurity programs checked from autonomous sources. Discuss on how different associations are being hacked and are protecting themselves, likewise establish and manage relationships with appropriate national and local authorities for cyber-crime responses.

4. **Directors shall guarantee management executes a good cyber-risk framework for the company**

Managing the company varies from organisation to organisation. There mustn't be a conflict of management among the board members and therefore the managing workers. They must decide what share of the profit is to be used for IT purposes and what for security. Under no circumstance shall cybersecurity be neglected.

5. **The board shall assess cyber-risk like any other enterprise-level risks:**

The board should audit attainable risks and the way to avoid, mitigate and insure against them. A report of cost per record of data breach and applied information must be made to ensure cyber insurance risk coverage is adequate to address potential cyber risks.

The Institute of Internal Auditors (IIA) The Information Systems Audit and Control Association (ISACA) The National Association of Corporate Directors (NACD) and The Internet Security Alliance (ISA). These are a few of the main organizations that have been working on issues of corporate governance with respect to cybersecurity.

NACD and ISA published a report titled the "**Cyber-Risk Oversight**" which also suggest certain questions which should be discussed in board meetings.

"The board of directors needs to be aware of the considerable resources taken to investigate each privacy issue based on federal or state regulations. So when there is a potential issue even if it's a misdirected fax a formal investigation has to occur and this does consume resources but it's a very important part of patient privacy", this was said by Shawn DeGroot, who is a Certified Healthcare Compliance Fellow (CHC-F), Certified Compliance & Ethics Professional (CCEP), Certified Healthcare Research Compliance (CHRC), Certified Healthcare Privacy Compliance (CHPC) and the ex-President of Health Care Compliance Association (HCCA).

 [ISSN 2581-5369]

V. ROLE OF COMPANIES IN CYBERSECURITY: THREAT BRIEF

Data protection is concerned with the ways that third parties handle it, the knowledge they hold concerning us- how it is collected, processed, shared, stored and used.

Data brokers, these businesses specialize in making in-depth profiles from people's data for advertisement. A single profile may draw up to 1,500 data points. This includes a person's sexuality, family, friends, browsing history, personal preference, political affiliation and even medical records. One US-based data broker Acxiom claims to own files on 10% of the world's population. In 2013 Edward Snowden revealed mass government surveillance programs, opening a global conversation which is still unfolding today. These pieces of information can be used to map people's psychology, likes, dislikes, your day-to-day lifestyle pattern, exploiting your domain of privacy by data analysis.

The way companies make profits is through internet business model. It depends on people sharing their personal data in exchange for access to content, services and social media platforms. You may not pay anything directly to go on Facebook they still make money by capitalizing your personal information to advertisers. Every website you visit has a checkbox for agreeing to their terms and conditions. By clicking on that, users technically consent to the current model and to look at the practicality of it, no one really reads any of the terms and conditions. This is a problem because nobody is aware of what they are really signing up for, which creates opportunities for manhandling the data you feed the website with. One search on google floods all your internet platforms with similar advertisements. The search results fro every individual is different on the same platform. Google has a vertical search bias which allows it to crawl and index the search results best suited for you. Google has been sued twice by the U.S and EU for violating Anri Trust Laws. You can search for any product on Google, the first link it will offer you is Amazon. It is because Amazon has paid Google for being at the top of any other shopping platform. Byjus has a tie-up with Facebook wherein Facebook gives its users random quiz if you have kids, if yes then how many, how old are they, and so forth. Facebook then sells this information to Byjus. Byjus now knows exactly who to target and with what learning package. These companies buy and sell data to know their potential customers and target them. This proves how the entire web is interlinked where one leak may tarnish your complete privacy.

Another challenge relates to the gathering of personal data by governments. There are not only companies who are hungry for data, even governments across the globe sit like vultures to grab any piece of information they can get their hands on. Technological developments now enabled

governments to monitor our conversations, transactions, uploads, and the locations we visit. In some countries including Russia, Brazil, Australia and South Korea- companies are legally required to store these data locally for a long period of time, making it easier for governments to get information on their citizens. These measures are often introduced in the name of fighting cybercrime and terrorism, which has been proved wrong by various studies. There has been no change in terrorist attacks or in some cases only increased. A logical reason for this being, the terrorist crews have equally skilled hackers working for them who can predict potential risks and work accordingly. Without adequate protection, this data can be easily abused to target dissidents and activists- undermining freedom of expression and the right to association and assembly. This has become a major point of discussion in India since the CAA protests started. These are just the technologies we are currently using. Technological advancements are only going to make data breach easier. Electronic wearables and artificial intelligence are likely to pose new challenges in case of cybersecurity.

Companies need to strengthen their corporate governance on cybersecurity and not depend on the government for it. Companies hold valuable data which can be used by the government with malafied intentions as has been proved in case of the US NSA by Edward Snowden. In the case of *Apple vs. FBI*, where FBI in 2015 was unable to crack the passcode of the accused, they asked Apple to create a unique OS just for the accused phone. Apple declined stating, "In the wrong hands, this software- which does not exist today- would have the potential to unlock any iPhone in someone's physical possession." These issues extend not only to individual phone theft but also hostile governments around the world exploiting this back door.

VI. GDPR: IS INDIA READY FOR SUCH A LAW?

After the Cambridge Analytica data hacking case reported in March 2018, the European Union (EU) enacted the GDPR 2016. As a result, e-commerce companies registered in non-European jurisdictions are subject to a legal framework on par with these regulations[12].

GDPR has two access points, the first one is the controller i.e the one who asks for data. It must be told as to how the data will be used. Second, is the Processor i.e the one which is being asked for the data. The processor cannot use to mine data in such a way to hit into anyone's privacy.

Most Data processing is done in India, India receives huge IT outsourcing from other nations in view of low costs which makes us obligated for information from different parts of the world.

[12] https://www.deccanherald.com/business/economy-business/gdpr-and-its-impact-indian-700371.html.

 [ISSN 2581-5369]

GDPR would affect the administration segment, particularly segments like information passage, client care, promoting, banking and IT, among others. Indian companies dealing with European customer will not be allowed to continue dealing with EU citizens until the Indian information insurance laws are viewed as sufficient and in line with the GDPR rules. If an Indian company uses data of former European customers, it would be liable for penalisation under the GDPR.

GDPR criteria to be complied by for Indian companies:-

- Presence in an EU country
- No presence in the EU, but it processes personal data of European residents
- More than 250 employees

GDPR specifically confers protection to citizens and rights to decide on how their data is processed which is not expressed anywhere in the IT Act. The principles stated in the GDPR apply to data processing norms. However, the principles under the IT Act 2000 apply to the collection of information and its use. Principles listed in the GDPR but not mentioned in IT Act are data integrity, protection from unlawful processing, accountability, fairness, transparency and in general protecting privacy of the Indian citizens.

India's weak data protection laws may become a reason for loss of business in the European market and increased cost of compliance. If there is a possibility of any liability arising on the Indian Company, there is a need for the Board of Directors to make an assessment and disclose the risks that may arise from the point of view of Corporate Governance companies must disclose their "GDPR Risk Liability" in their shareholder disclosures from the next financial year.

VII. CONCLUSION

Cybersecurity issues and privacy issues were looked at as only Information Technology issues, but in today's time, it isn't so. Unlike other countries, India has been sleeping over cyber threats posed by organisations that have become a household name. Bigger the company higher the risk. It is not just the general public which needs to be protected against misuse of their data but also organisations from external hacking attacks which is the reason it makes it an important issue in corporate governance. Settling for cheap in data protection programs will take a toll on the functioning of the organization. Disclosure of information, destruction of data, losing credibility are just a few repercussions an organisation may face if it happens to face a cyber attack.

 [ISSN 2581-5369]

With the growing technological advancements, the types of cyber risks are getting more sophisticated which make it extremely necessary and the need of the hour for corporates to come up with cybersecurity policies and also to have their data insured by way of cyber insurance.

Due to a lack of laws pertainig to cybersecurity, India is open to a huge risk of data breach. The European countries follow strict laws regarding data protection, the laws in EU countries are so diligently followed that they are even used by international courts. The burden of cybersecurity is on the IT Act which deals with data protection, Shri Krishna committee which only gives guidelines. No substantive law to regulate data or regulating controllers. The government should now focus on how to make futuristic laws generating from EU countries.

*****

 [ISSN 2581-5369]