VOLUME 4 | ISSUE 3

INTERNATIONAL JOURNAL OF ADVANCED LEGAL RESEARCH

IMPORTANCE OF DATA PRIVACY AND CYBERSECURITY

- Harsh Rawat[1]

ABSTRACT:- The paper discusses the importance of data privacy and cyber security, covering the data privacy lawsin India and its application. It discusses the ambit of data privacy on the lives of individuals, its nature and its protection from cyber-attacks. Data privacy and its protection are needed for several reasons which include better protection of individual data, building trust amongst the people, increasing digital exposure, increased frauds, data breaches, among others, etc. Data is wealth in this tech generation. The importance of data cannot be denied. The requirement for data privacy has led to the implementation of different laws and regulations by the governments of different countries, regulating data security. Some major data protection laws include the General Data Protection Regulation in the EU, the California Consumer Privacy Act in the US, the Digital Personal Data Protection Act in India etc. Such laws may vary according to different regions and requirements but most of them have similar requirements.

The concept of data privacy is not very new. In India, various data protection laws have been passed by the Parliament and many initiatives have been taken by the government to ensure cyber security. Cyber security can be utilised as an effective governance tool to mitigate and prevent any sort of cyber-attacks and data infringements. It included many strategies that can be used by any organisation, company or even the government to prevent any data breach. Generally, for the effective implementation of any rule or regulation, a holistic effort is required, and cyber security is no exception. Individuals need to be vigilant regarding data privacy, and should quickly take action if any data infringement incident happens with them.

KEYWORDS:- Data Privacy, Cybersecurity, Cyber-attacks, Data Infringement, Cyberspace, Data Protection.

(A) INTRODUCTION:-Data privacy has become an important part of our daily life. It refers to the preservation and protection of an individual's data from any sort of

[1] 3rd Year Law Student at Dept. of Law, PIMR, Indore

unwarranted breach and to prevent it from unauthorised use, access, disclosure, destruction, or modification[2]. It demonstrates that only the personal information of an individual is collected and is only used for official and legal purposes. It ensures that people have control over their personal information, thereby protecting their privacy from getting infringed without their authority or permission. It also involves that personal data collected from the individual is obtained through a legitimate process. The data collected in this process must be correct, absolute and properly updated. That is properly handled and stored securely[3]. The term data privacy is broad. One of the subsets of data privacy is cyber security. Cyber security deals with the protection and preservation of data from illegal access and cyber-attacks by hackers, or kind of malicious software[4]. It encompasses mechanisms like applying strong password policies, data encryption to preserve data at both transits and at rest, use of firewalls, updation and use of patching software to curb the vulnerabilities associated with data security and use of other cyber security measures to stop unauthorised encroachment and any access to data system and networks. Cyber security also includes surveillance and monitoring for any sort of security threats, and showing due diligence in response to any such incidents that may occur to reduce the effect[5]. Thus, both data privacy and cyber security are very essential for securing the information of individuals and ensuring integrity and security in the digital world[6].

(B) RESEARCH METHODOLOGY:- The research paper is descriptive in nature and consists of both quantitative as well as subjective information. Mostly, secondary sources of research like articles, websites, research papers, journals and blogs are utilised for this research.

(C) REVIEW OF LITERATURE:-

[2] Stephen J Bigelow, *data Privacy(information Privacy)*, Tech Target (Feb 4, 2024), https://www.techtarget.com/searchcio/definition/data-privacy-information-privacy

[3] *Data protection and privacy laws*, Worldbank.org, (accessed Feb 2, 2024),https://id4d.worldbank.org/guide/data-protection-and-privacy-laws

[4] *What is Cyber Security*, Kaspersky(accessed Feb 2, 2024), https://www.kaspersky.co.in/resource-center/definitions/what-is-cyber-security

[5] *The Five Functions*, NIST, (accessed Jan 30, 2024), The Five Functions | NIST

[6] *Importance Of Data Security In 2024- Why Is It Important?*Intellipat, (accessed Feb 6, 2024), https://intellipaat.com/blog/importance-of-data-security/

1. **Data Privacy And Cybersecurity** by Kamshad Mohsin[7], (Assistant Professor, School Of Law, Maharishi University Of Information Technology). The above-mentioned study discusses the importance of data privacy and how it is ensured through cyber security. It discusses the necessity of data privacy in the cyber world. It highlighted the cyber security rules and regulations that aim at ensuring data privacy. Further, it discusses various data privacy laws as well as provides additional safeguards for private individuals regarding data security.
2. **Cybersecurity Is Critical for All Organisations – Large & Small** by IFAC[8]. This study discusses the significance of cyber security and its huge impact on the lives of the people. It deals with cyber security governance, which can be used as an effective tool by any organisation, company or government to ensure data privacy of their system. It discusses various strategies and steps that can be taken to mitigate the risk of cyber-attacks.
3. **Data Protection And Privacy – Cybersecurity Laws In India** by King Stubb &Kasiva[9]. This study discusses the various cybersecurity laws of India and their application.

(D) NECESSITY OF DATA PRIVACY IN THE CYBERSPACE:-

In the current time, most of our personal information is stored digitally and transmitted through digital platforms. It comprises one's financial information, personal identification details, medical records and other sensitive information[10]. Such information is stored online on various devices like computers, mobile phones, cloud servers and others. It is quite important as well as utmost necessary to have reliable data privacy and cyber security policies that are strong enough to secure this information from unwarranted attacks or infringements. Data privacy is thus indispensable for ensuring the secrecy and integrity of the customers or individual data. Its availability and proper make sure that the personal

[7] Kamshad Mohsin, *Data Privacy And Cybersecurity*, Papers.ssrn.com, (accessed Jan 28, 2024), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4299439

[8] Steve Ursillo, JR., Christopher Arnold(2023), *Cybersecurity Is Critical For All Organisations – Large And Small*, International Federation Of Accounts(IFAC), (accessed Feb 08, 2024), https://www.ifac.org/knowledge-gateway/preparing-future-ready-professionals/discussion/cybersecurity-critical-all-organizations-large-and-small#:~:text=Cybersecurity%20is%20making%20sure%20your,from%20unauthorized%20access%20or%20damage

[9] King Stubb & Kasiva, *Data Protection & Privacy – Cyber Security Laws In India*, kSk Advocates And Attorneys, (accessed Feb 8, 2024), *https://ksandk.com/information-technology/cyber-security-laws-in-india/*

[10] Nass, S. J., Levit, L. A., Gostin, L. O., & US), M.(2021), *The Value And Importance Of Health Information Privacy*, Nih.gov, (accessed Feb 6, 2024), https://www.ncbi.nlm.nih.gov/books/NBK9579/

information of the individual is protected[11]. It comprises things like data encryption, carrying out strong password policies and constantly renovating the security measures to remain ahead of any future threats and cyber-attacks. The need for data protection and data privacy[12] can be summarised as follows:

- **Ensures protection of personal and other information of individuals:-** The objective of the data previously lost focused on ensuring genuine protection of the personal as well as non-personal information of the citizens of the country. First of all, such laws were focused on regulating the manner of collection and processing of information, analysing the grounds of consent of the individuals. Penal provisions attract penalties in case any company do not safeguard the information in compliance with the law etc.
- **Builds greater trust amongst individuals:-** These laws are necessary as the health in making a stronger core for trust and credence among the people. When the entities emphasise onprioritising the privacy and protection of their users' data and thereby handle their data meticulously, it demonstrates their dedication towards the protection of personal data which aids the consumer to develop and build a strong relationship with the company.
- **Maintenance of Right to Privacy:-** As we have already discussed, the Constitution of India recognises the Right to Privacy of an individual as a fundamental right under Article 21. It means that each person has an inherent right to their data. It provides them the right to decide how their information be used and when they decide to retract their consent or oppose the processing of their data.
- **Increased Digital Presence:-** A major portion of the population of the Indian subcontinent is now connected to the Internet. With the widespread use of social media platforms such as Instagram, Facebook, Twitter etc., people are leaving their digital footprints all over the Internet. If such things are not handled correctly, it can lead to a considerable amount of data breaches.

[11] Andrea Gil, *Data Security - Confidentiality, Integrity & Availability*, KVA by UL, (accessed Feb 4, 2024), https://www.kvausa.com/data-security-confidentiality-integrity-and-availability/

[12] Adv. Komal Arora, *Data Protection & Data Privacy Laws In India*, Ipleaders, (accessed Feb 6, 2024), https://blog.ipleaders.in/data-protection-laws-in-india-2/#:~:text=The%20need%20for%20data%20protection,non%2Dpersonal%20information%20of%20citizens.

- **Absence of Consciousness:-** The sheer lack of awareness of data protection also becomes another ground to have such a law in our nation. People use mobile phones all the time. Yet, they are unaware of the law that regulates and governs the Internet system They are also not able to realise the results of their actions while using the Internet. Thus, a law is necessary that would create awareness among the public regarding the importance of privacy on online platforms so that it would be convenient for the administrative authorities to educate the people concerning their rights and duties during the time they are active on online platforms.
- **Aids in stopping data breaches, identity thefts etc:-** With the rapid expansion of Internet facilities being accessible at every household, there is a high probability of commencement of any offence such as identity thefts, fraud, data breaches, etc. Data protection and privacy laws would play a very important part in placing such mechanisms that would assist in the prevention of such offences.

- **Promotion of Economic Growth and Innovation:-** Data protection and data privacy have become so important in today's time that without them, a country cannot achieve economic growth. They have emerged as a requisite for the development of a nation and thus ensure security in case of any breach of data. Now, a greater number of countries as well as enterprises would like to invest in those companies where the data protection and privacy framework is powerful.
- **Securing Children's Privacy:-** In today's digital age, most children have become virtually active on all digital platforms because of which the need has emerged for special laws and policies that would make sure that any data infringement is not happening. Kids are more prone to consent to any permissions the results of which they are unaware. Special attention is needed in this regard. Also, some games might require children to provide diverse information about themselves to play the game of whose ramifications they are unaware of. A systematic law is thus needed which would ensure proper protection of data and also raise awareness about it.
- **Data Principles or Ethics:-** Data privacy and cyber security laws not only serve the objective of data collection and processing but also data ethics. Data ethics are the morals or the principles that ensure that the collection of data and its effective processing must be based on ethical criteria i.e., the data processing must be transparent, not forceful, fair and non-discriminatory.

- **Safeguarding Individual's Rights:-** These laws aim to empower the individual in not just one way but in many ways. With this, they get a right to have information of their data, its storage, collection and transfer and also the right to remedy in case of any violation. Individuals must be fairly reimbursed for any data infringement. In this way, an effective complaint redressal mechanism has come into existence.
- **Facial Identification and Inspection:-** Modern technologies such as facial identification and surveillance have emerged which from time to time have raised many concerns regarding the privacy of individual data. This law would aid in rooting out such problems and to ensure more accountable data collection methods by the individuals.

Thus, overall, we can infer that data Protection and data privacy regulations are of prime significance because they make sure that an individual's private data is safe and secure in this tech universe. Data is a very valuable asset, and its importance cannot be denied. This is the age of data revolution. Any individual's data should not be used or processed without his or her express consent. In case any data breach occurs,appropriate legal action must be taken in consonance with the data protection laws of the country. If there is no law in place, then the offender would have easily escaped.With the effect of this law,now, the government sector as well as the private sector are obliged to comply with its provisions.

(E) EVOLUTION OF DATA PRIVACY LAWS:-

The concept of data privacy is not very new. It has been in existence since the case of Semayne in 1604[13]. The notion of data privacy developed thereafter. Further, the Universal Declaration of Human Rights(UDHR) also elaborated on individual privacy under Article 12(4).

Privacy has always been a matter of discussion and debate in Indian society in judicial courts, with few considering privacy as a fundamental right while others did not accept it as a right under the Constitution of India. Eventually, in 2017, in the case of KS Puttusamy Vs UOI[14], it was held by the Apex Court of the country that the right to privacy is a fundamental right under Article 21[15]of the Constitution of India. Although there was the IT Act, 2000 that includes privacy, there was inadequacy of any independent and extensive law on such

[13](1604) 5 Co Rep 91a : 77 ER 194.
[14]K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1.
[15] INDIA CONST. art. 21

subject. Over time, after 7 years of making and 3 endeavours to move the privacy law, India espoused a fully developed data privacy and protection law on August 9, 2023.

When we discuss data privacy laws, we usually mean those laws that control the use, collection, revelation and security of personal data and information[16]. Such laws are intended to secure and safeguard individual's private information and to make sure that it is only used, collected and revealed for legitimate purposes only. Based on country or region, data privacy laws vary but a majority of them have identical principles and requirements. For instance, a lot of data privacy laws require organisations and companies to secure individuals' consent before using or collecting their private data to give individuals control over their data and to further make sure that their information is stored and handled securely[17]. This can comprise things like providing people the right to access their personal information,the right to rectify any inaccuracy in their data and the right to delete their data on request. Data privacy laws normally require that organisations and companies should be transparent and honest in collecting using disclosing any personal information of any individual and to supply people with clarity of information regarding their privacy rights and alternatives.

Some prominent examples of data privacy regulations comprise the General Data Protection Regulation(GDPR), which is applicable in the European Union and the California Consumer Privacy Act(CCPA), which is applicable in the United States of America[18]. Let us discuss some features of these regulations:-

General Data Protection Regulation (GDPR):- GDPR is a data protection law that was embraced and adopted in 2018 by the European Union. A defined set of rules and guidelines were established by this regulation for the objective of collection, protection and the use of personal data of people in the European Union[19]. The key points of the GDPR are the following:

[16] Osano Staff, *Data Privacy Laws: What you Need To Know In 2024,* Osano, (accessed Feb 4, 2024), https://www.osano.com/articles/data-privacy-laws

[17] *What's Data Privacy Law In Your Country,* Privacy Policies, (accessed Feb 6, 2024), https://www.privacypolicies.com/blog/privacy-law-by-country/

[18] Danielle Kucera, *CCPA vs GDPR: Similarities & Differences Explained,* Okta.com, (accessed Feb 2, 2024), https://www.okta.com/blog/2021/04/ccpa-vs-gdpr/

[19] *EU General Data Protection regulation (GDPR),* Trendmicro.com, (accessed Feb 2, 2024), https://www.trendmicro.com/vinfo/in/security/definition/eu-general-data-protection-regulation-gdpr#:~:text=What%20is%20the%20EU%20General,which%20was%20adopted%20in%201995

- All organisations and companies are now required to obtain prior permission from individuals before collecting their personal information. They are required to provide clear and easy instructions regarding how they will process the individual's data.
- It provides the right to access one's data to an individual. It also provides the right to request to an individual for removal or modification of their data, and also the right to object to the processing of their data.
- The companies and the organisations are required to implement suitable organisational as well as technical measures to secure the private data of an individual against any unacceptable access, collection, disclosure, use or destruction.
- The companies and the organisations are required to notify private individuals and the concerned authorities in case any breach of data occurs.
- A set of noteworthy fines and penalties have been imposed on the organisations and the companies in case of any failure to abide by any of the policies and requirements of GDPR.

GDPR, in general, is a deliberate attempt to provide individuals with greater authority over their private data and to make sure that all companies and organisationsmanage and deal with the sensitive data of the individual in a transparent and accountable manner.

California Consumer Privacy Act (CCPA):- CCPA is that data privacy law that was passed by the state of California in 2018. It applies to those businesses and entities that use and collect the private data of citizens of California and those who fulfil a certain criterion, that is having yearly gross revenue of more than $25 million, or buying or disposing of the personal data of over 50,000 customers or devices per year; or obtaining more than 50% of the business yearly revenue from selling or disposing the personal information of individuals. There are some key provisions of CCPA[20], which are as follows:

- A requisite for businesses to reveal their methods to the consumers regarding how they collect the personal data of individuals. Purpose of obtaining and with whom they are going to share it or disseminate it.
- Consumers have the right to choose out of selling of their data.

[20]*California Consumer Privacy Act (CCPA),* State Of California Department Of Justice, (accessed Jan 31, 2024), https://oag.ca.gov/privacy/ccpa

- Right to request for deletion or alteration of one's data.
- The act requires businesses to adopt and implement appropriate security measures to protect the individual's private information.
- Penal provisions have been made that would make sure that no enterprise will be allowed to disobey this regulation. In the case of any non-compliance, the businesses are required to pay the penalties.

In summary, the CCPA was made to give customers greater control over their information and to hold any business entity responsible for their management of personal data.

(F) DATA PROTECTION AND DATA PRIVACY LAWS IN INDIA:-

1. **Overview of Information Technology Act, 2000:-** The IT Act, 2000 that came into enforceability in 2000 was amended in 2008. One of the most prominent sections of it was section 43A[21]. According to it, if a corporate body dealing, possessing or handling very sensitive data or personal information of an individual turns negligent in showing and securing proper security during the process, which would amount to wrongful damage, then such corporate bodies are bound to pay damages for such wrongful loss. Moreover, there are Information Technology (Reasonable Security Practises and Procedures and Sensitive Personal Data orInformation)Rules, 2011 which specialises in the protection of sensitive data of individuals like bank details, medical information and related records, etc. Section 72A[22] of the ITAct specifies the punishment as well as the fine that goes up to Rs 5,00,000 or imprisonment for a term which may extend up to three years in situation of disclosure of personal information intentionally and knowingly without taking due permission from the concerned person, thereby breaching the conditions of a lawful contract.

2. **Overview of Digital Personal Data Protection Act, 2023:-** The DPDP Act is a very recent legislation for the effective processing of personal data in India. Section 2[23] discusses various definitions relating to data fiduciaries, data principles etc.It was eventually adopted nearly 6 years after the Apex Court of the nation recognised and upheld the right to privacy as a fundamental right under Article 21 of the Indian

[21] Information Technology Act, 2000, § 43A, No. 21, Acts Of Parliament, 2000 (India).
[22] Information Technology Act, 2000, § 72A, No. 21, Acts Of Parliament, 2000 (India).
[23] Digital Personal Data Protection Act, 2023, § 2, No. 22, Acts Of Parliament, 2023 (India).

Constitution. This act is formulated against the backdrop of different privacy laws around the world like the California Consumer Privacy Act (CCPA), and the European Union's General Data Protection Regulation (GDPR) and hence, it deals with privacy and safeguarding the obligations regarding the private data. It is believed that the Digital Personal Data Protection Act have borrowed some concepts and policies straight from the GDPR and it has a broad scope of applicability that extends beyond the territory of India. On one hand, the above act imposes a very firm obligation for the illegal processing of private data,on the other hand, there are many noteworthy exceptions for the government authorities. A comprehensive framework was established by the DPDPAct for the duly processing of individual personal data and thereby substituted the provisions of the Information Technology Act. There are some features of the DPDP Act which are as follows:

- **Bodies constituted under the DPDP Act:-** The act makes use of different terms which may appear very perplexing in the beginning. It is very essential to acknowledge the nature and differences between the terms used like data fiduciaries, data processors, data controllers, data principle etc. An individual whose personal information is used and collected is called the data principal while a data fiduciary is the body that determines the means and the purpose behind the processing of personal information. Their designation is similar to that of a data controller.
- **Exceptions Recognised Under DPDP Act:-** These are certain exceptions that are allowed in the interest of the sovereignty and integrity of India, the security of the country, amicable relations with foreign countries, maintenance of public order and peace and averting any incitement to commit the offences, etc, are allowed and recognised under DPDP Act.
- **Application of DPDP Act:-** This act has extra-territorial jurisdiction and application, and it has no limitation on international data transfers.
- **The rationale behind the lawful processing of personal data:-** One of the primary sources for the lawful processing of personal data of an individual is consent. Further, a legitimate claim can be identified by the data fiduciaries for the lawful processing of personal data.
- **Personal Data Individuals Rights and Obligations:-** There are certain rights for data principles, including the right to erasure, right to access and right to object.

The subjects are also required to obey certain obligations, the non-compliance of which may result in fines as well as punishment for a definite term.

(G)CYBERSECURITY RULES & REGULATIONS THAT AIM TO ENSURE DATA PRIVACY:-

There are so many cyber security laws and rules in the world that provide for data privacy. These laws may vary in terms of different regions, but many of them have identical requirements and provisions[24]. As discussed earlier, the General Data Protection Regulation(GDPR) of the European Union provided a set of rules and regulations regarding the use, protection and collection of private data of people.

In the same way, the CCPA has exclusive jurisdiction to regulate businesses in the USA about any data privacy compliance. When we take into account the Indian scenario earlier, there were no specific laws governing data privacy. Nevertheless, the legal matters regarding compensatory measures and penal provisions are dealt with exhaustively in the IT Act of 2000 which describes the scope of the data privacy laws in India, along with the Indian Contract Act, of 1872. The Personal Data Protection Bill, 2019 was passed by the Indian parliament which seeks to ensure the protection of private data of individuals and led to the formation of data protection authority for that purpose. This will govern the processing of the private data of individuals by the companies incorporated in India, foreign entities that deal with the private data of citizens of India and the government.

Further, section 72A of the Information Technology Act, 2000 provided for stricter penal provisions related to any wilful or accidental dissemination of private data of an individual in breach of a lawful contract which would be considered a punishable offence that would attract a fine amount of up to Rs 5,00,000 along with imprisonment for a term which may extend to three years or both.

Section 72[25] of the IT Act, 2000 also provided the penal provisions related to breach of confidentiality of personal data of citizens of India. It states that if any breach of personal data of individuals is caused by any lawful authority, then the individual acting as a lawful authority will be held responsible for such breach of data privacy and thus will be held liable

[24] *Cybersecurity & Privacy Laws(2016),* Itgovernanceusa.com, (accessed Feb 7, 2024), https://www.itgovernanceusa.com/federal-cybersecurity-and-privacy-laws

[25] Information Technology Act, 2000, § 72, No. 21, Acts Of Parliament, 2000 (India).

for imprisonment for a term which may extend to 2 years or with fine, which may extend to Rs 1,00,000 or both.

The Information Technology (Amendment) Act, 2008 has brought a revolution to the concepts of the Indian Contract Act, 1872 through the introduction of E Contracts. It has amended Section 43A and Section 66[26] Of the IT Act. Section 66 provides penal provision of the offence that may involve punishment for a term which may extend to three years, or a fine up to Rs 1,00,000 or both.

As discussed earlier, the Digital Personal Data Protection Act, 2023 was also passed by the Indian parliament for the effective processing ofdata of citizens of the country. Also, a comprehensive framework was set up by the DPDP Act for the duly processing of individual personal data and thereby substituted the provisions of the IT Act. The right to privacy is also part of the fundamental rights of citizens under Article 19[27] and Article 21 of the Indian Constitution. Many steps have been taken by the Government of India to make sure that the data collected of private individuals by social media platforms and hardware devices is not misused and is only done in conformity with the cyber security laws of the country to avert the breach of any personal information of people from any cyber-attacks.

Let us discuss some of the initiatives taken by the government of India on Data Privacy and Cybersecurity.

- **Cyber Surakshit Bharat:-** This programme was commenced by the government to make a strong cybersecurity ecosystem in the country.
- **The Indian Computer Emergency Response Team (CERT-In):-** It functions as the country's national agency to tackle cyber security occurrences. It is also responsible for reducing the number of cyber infringements on government networks and databases.
- **National Critical Information Infrastructure Protection Centre(NCIIPC):-** This centre was established by the central government to secure the sensitive information of the country that may have a huge impact on the unity and integrity of the country, national peace and security, public health care and economic growth.
- **Provision For The Appointment Of Chief Information Security Officers(CISO):-** The Government of India has issued a written guideline for CISOs of all the

[26] Information Technology Act, 2000, § 66, No. 21, Acts Of Parliament, 2000 (India).
[27] INDIA CONST. art. 19

government departments laying out the best practices for protecting apps, their infrastructure and their adherence. The CISOs have the authority to identify and record any security requirement that may originate within a technological innovation.

- **National Cybersecurity Policy, 2013:-** The main objective of the policy was to create safe and secure cyberspace for the citizens, the company and the government. The Mission also included developing cyberspace and the infrastructure in such a manner so that it remains unaffected by any sort of cyber-attacks or infringements and to reduce any loss through coordinated efforts of the people, institutional structures, technology etc. The Cyber Swachhata Kendra(Botnet Cleaning & Malware Analysis Centre) was created to meet the goals of the National Cybersecurity Policy that provides for the growth of secured cyberspace in the country. This policy also aims to create a workforce of 5,00,000 cybersecurity professionals in the coming five years through skill development, capacity building and training. It emphasises on creating an effective mechanism for cyber-crime prevention, prosecution and investigation, as well as evaluating the capabilities of law enforcing authorities.

Thus, there are so many rules and regulations that require companies andorganisations to getindividualconsent before gathering their personal information to give individuals control over their details against any unauthorised use, access, dissemination or destruction[28]. Most often, they can also impose massive fines to abide by their terms and conditions.

(H)CYBERSECURITY GOVERNANCE:-

We have all discussed various laws and regulations dealing with data privacy and cyber security prevailing in the world as well as in the Indian context, and also the initiatives taken by the Indian government regarding cyber security. Now, we would look at and try to understand how cyber security can be used as an effective governance tool in preventing any sort of cyber-attacks in data privacy. This kind of tool or a governance strategy helps an organisation company as well as government to better manage the data collected and used by all of them.

The need for cyber security must be considered along with the risk associated with it by the owners of any organisation or company. It should be at the same level as operations, compliance, finance and goodwill risks with appropriate management standards. Its results must be properly monitored and controlled.

[28]*Data Protection & Privacy: 12 Ways To Protect Users Data,* Cloudian, (accessed Feb 8, 2024), https://cloudian.com/guides/data-protection/data-protection-and-privacy-7-ways-to-protect-user-data/

Protection From Malicious Software And Other External Attacks:- Some mitigation strategies to protect the organisation from malicious attacks are:

1. Use of firewalls which are designed to safeguard the system from any cyber-attacks by hackers from accessing an organization's data system by both external as well as internal communication links.
2. Spyware and web proxy defence solutions preserved the system from any software code from any pop-up window that may have deceitful intent such as logging passwords and user names for committing frauds.
3. Use of anti-spam and anti-phishing software for blocking spam messages and tracking websites made for fraudulent purposes.

   The above-mentioned strategies are very necessary to ensure protection from any cyber threats. The magnitude of a cyber-attack can be huge, involving significant loss of data, cost of reconstructing the system, etc.Such cost,however, must be taken into account by an organisation before analysing such cost against the cost incurred in establishing a cyber security defence system.

Hardware Maintenance Policies:- The maintenance contracts must be continued with the suppliers of hardware so that, in case of any failure, it can be rectified quickly. Such a contract should specifically mention the service levels that will be meted out by the supplier in case of any failure. Some important hardware such as servers, backup technologies and switches require quick attention. An organisation that depends uponmaintenance contracts should ensure that the supporting company is maintaining a sufficient quantity of spare components to satisfy the service level commitments of the organisation. Moreover, the standard of the external IT support company of the organisation will be critical to make sure that the security mechanisms are correctly supported and implemented.

Documentation & People:- Every organisation should have a well-defined plan to alleviate the risk of important people being inaccessible in case of a system failure. Every organisation must maintain a list of contact information for backup technicians. Documenting the hardware configuration as well as the software applications, and keeping it up to date is of prime importance to ensure that new technical professionals do not face any difficulty in rebuilding the system.

Governance Procedures And Policies:- Appropriate IT regulatory procedures must be made in an organisation. It is also critical to implement a formal risk assessment mechanism and to develop suitable policies to make sure that the systems are not wrongfully used. The IT policies must be reviewed regularly and properly updated to identify any current threats. It comprises developing response procedures and policies to adequately respond to and to help diminish the cost of potential breaches. The timing and education regarding technological risk must form part of an organisation's risk management strategy. Policies must include these things:

- Individual account management;
- Data Management including managing repositories, data recovery and backup, and appropriate dissemination of data;
- IT Cybersecurity & risk management practices.

Some general policies adopted by the organisations are as follows;

a. **Email Use Policy**:- Elements of this policy include-
   - Forbidding the use of private email accounts for company matters.
   - Forbidding opening of any email attachments from unspecified sources.
   - Prohibiting any distribution of one's email passwords.
   - Forbidding access to other people's email accounts.
   - Notification Of Email monitoring by the organisation.

b. **System Use Policy**:- This policy defines the rules by which an entity's IT system can be used. Elements of this policy comprise:
   - Compulsory use of passwords on all the systems like mobiles and tablets as well as the need to change the passwords continuously.
   - Prohibiting any act of copying or removal of the organisation's data without approval.
   - Encryption of data as well as security of equipment.
   - Rules for the use of the system for business hours and outside business hours. Verification of user's identity using multifactor authentication.

c. **Internet Policy**:- Some elements of this policy include-
   - Use of the Internet for business purposes.

- Forbidding access to offensive websites.
- Ensuring safe downloads and tracking of internet usage
- Limiting the spam by prohibiting access to user's email ids.

d. **Remote Access Policy**:-Some important elements of this policy include:-

- Approvals are made mandatory for external access.
- Compensation for any external access costs.
- Physical security of equipment of organisation.
- Reporting of any data infringement of the organisation.
- Organisations can monitor any suspicious activity or unusual usage patterns of their users through agreement.
- Dispute resolution.

Insurance:-Suitable insurance must be obtained by any organisation or a company to cover the replacement cost of damaged infrastructure and labour costs, and also to inquire into the matter of restoring data and rebuilding systems. Insurance must take into consideration the loss of productivity as a consequence of massive system failure or disastrous event.

(I) CONCLUSION:-

There are so many ways through which an organisation or a company can ensure user privacy through cyber security. Some important steps that can be adopted to ensure data privacy include:

- Obtaining due constant from the individual whose details are collected, and providing specific instructions in simple terms about usage of their private data.
- Implementation of suitable organisational and technical measures made by the organisation to secure the personal information against unauthorised use, disclosure, access or destruction. It can comprise elements such as strong password policies, data encryption updation of software, use of firewalls and other security mechanisms to prevent any breach of data.
- Providing individuals control over their data, such as the right to access, alter, and delete any personal information as well as the right to object regarding processing of their data.

- Proper surveillance and monitoring for any potential cyber-attacks and immediately taking responsive measures. It comprises things such as monitoring any unusual activities, conducting security audits and other measures that are immediately required.
- Sensitising and training the organization's employees about data privacy and cyber security measures and practises to make them understand their part in preventing other such data breaches.

INDIAN CONTEXT: The data privacy laws in India have witnessed a drastic shift in its model towards the growth of a secure technological domain, where the data privacy of the individuals is not infringed. The IT Act, Personal Data Protection Bill, 2019 and The Digital Personal Data Protection Act, 2023 have all comprehensively worked together in the direction of creating a secure social and technological arena in which the data of the citizens are not mistreated by hackers, social media and malicious software. With the imposition of stricter fines and rigorous imprisonment in situations of breach of confidentiality and disclosure of information of private individuals without consent, the government has effectively succeeded in deterring the violators and the cyber attackers from committing any such offences of similar nature.

Data privacy has become so important in our lives that, in the absence of it, one's data can be easily obtained and can be used for defrauding people. Ensuring data privacy is not a very simple task. It involves various tools and practices in averting any breach of data. Despitehaving so many data privacy regulations and a well-built cyber security system, the individual's data is prone to cyber-attacks. Thus, collective efforts are required from the individual users as well as the organisations to ensure privacy for the preservation of any disclosure of one's data. Overall, we can say that to ensure data privacy through cybersecurity, a combination of measures is required such as organisational policies, technical measures, employee education etc to secure the private data of individuals from unauthorised access.