Nishith Desai Associates
LEGAL AND TAX COUNSELING WORLDWIDE

MUMBAI SILICON VALLEY BENGALURU SINGAPORE NEW DELHI MUNICH / AMSTERDAM NEW YORK GIFT CITY

Research

Cybersecurity Law and Policy

Present Scenario and the Way Forward

July 2023

Research

Cybersecurity Law and Policy

Present Scenario and the Way Forward

July 2023

DMS Code: 21821.1

concierge@nishithdesai.com

FT INNOVATIVE LAWYERS 2019
FINANCIAL TIMES
ASIA-PACIFIC WINNER

Ranked as the 'Most Innovative Indian Law Firm' in the prestigious FT Innovative Lawyers Asia Pacific Awards for multiple years. Also ranked amongst the 'Most Innovative Asia Pacific Law Firm' in these elite Financial Times Innovation rankings.

Chambers AND PARTNERS

IFLR1000

The LEGAL 500

BENCHMARK LITIGATION

asialaw

WWL

ASIAN LEGAL BUSINESS

INDIA BUSINESS LAW JOURNAL

INDIA BUSINESS LAW JOURNAL THE LIST 2022 2023 LAW ASIA

Mergermarket An Acuris company

ITR WORLD TAX

ILA IDEX LEGAL AWARDS

LEGAL ERA BY THE PEOPLE. FOR THE PEOPLE. OF THE PEOPLE

concierge@nishithdesai.com

Disclaimer

Contact

For any help or assistance please email us on **concierge@nishithdesai.com**
or visit us at **www.nishithdesai.com**.

Acknowledgements

Gowree Gokhale
gowree.gokhale@nishithdesai.com

Vaibhav Parikh
vaibhav.parikh@nishithdesai.com

Mihir Parikh
mihir.parikh@nishithdesai.com

Aparna Gaur
aparna.gaur@nishithdesai.com

Aniruddha Majumdar
aniruddha.majumdar@nishithdesai.com

We would like to thank **Akhileshwari Anand** and **Raashi Vaishya** for their contribution to the paper.

We would also like to thank the following authors for their contribution to the sections on cybersecurity laws in their respective jurisdictions:

Nathan Salminen (Counsel) and **Paul Otto** (Partner), Global Regulatory Group, Hogan Lovells, Washington DC (US),
Tarryn Smith (Associate) and **Marc Dautlich** (Partner), Bristows LLP, London (UK),
Christian Saßenbach (Associate) and **Dr. Jürgen Hartung** (Partner), Oppenhoff, Cologne (Germany).

Contents

Introduction

The fourth industrial revolution, as popularly called, involves digitization in virtually every facet of our lives. From production and processing to storage and transactions, major sections of our economy have shifted online. With this digital shift, many enterprises as well as countries globally are facing cyber threats on a daily basis, making virtually everyone who has access to the internet a potential victim. On the other side, a variety of actors are behind cyber threats including terrorist organisations, criminal groups, hackers, malicious insiders and even hostile countries.[1]

According to Cybersecurity Ventures report, the damages inflicted by cybercrime are expected to reach $8 trillion globally in 2023 and increase to $10.5 trillion by 2025.[2] Global ransomware damages alone are expected to exceed $325 billion by 2031. Indian businesses and organizations are also affected by this trend. The reputed All-India Institute of Medical Sciences ("**AIIMS**") in India came under a ransomware attack which lasted over 10 days, and where medical records of millions of patients were compromised.[3]

In fact, with the increasing power of quantum computers, traditional encryption methods that are widely used to secure data may become vulnerable to quantum attacks. Hence, quantum computing is likely to aggravate cybersecurity issues in the future.[4] Moreover, several IoT devices possess inadequate security measures, rendering them vulnerable and easily exploitable by hackers.[5] Cybercriminals may also use artificial intelligence and machine learning technologies to plan more sophisticated and targeted attacks.[6] There are instances of Generative AI, for example, being reportedly used to create malware software code.[7] Even Deepfakes pose a significant cybersecurity threat due to their potential to deceive individuals and manipulate information.[8]

The Government of India has recognized the new age cybersecurity threats and has been taking multiple steps towards addressing these concerns. Institutions such as the Indian Computer Emergency Response Team ("**CERT-In**"), the National Cyber Coordination Centre ("**NCCC**") established by CERT-In, among others, are involved in collection of information on and mitigation of cybersecurity incidents. With the Digital India Act also set to be introduced, there might be further developments in the legal framework on cyber-security in India, continuing from the CERT-In's directions from April 2022.

In this paper, while the emphasis is on the Indian legal framework, we have briefly provided some context on cybersecurity issues and potential liabilities in Section 1. In Section 2, we delve into some cybersecurity laws in other jurisdictions. It is with this backdrop that cybersecurity law and policy in India is analysed in Section 3. Section 4 covers some key international treaties that India has signed with respect to cybersecurity co-operation and Section 5 provides key guidance for businesses and organisations with respect to their cybersecurity practices.

---

1 Imperva team, Cyber security threats, Learning Center, Imperva (2021), available at: https://www.imperva.com/learn/application-security/cyber-security-threats/, last accessed on May 30, 2023.

2 Morgan, Steve (2022, Dec 10) "Top 10 Cybersecurity Predictions And Statistics For 2023" Cybercrime Magazine., last accessed on May 24, 2023.

3 Sharma, P., AIIMS computers, Information Tech systems not upgraded for 30 yrs, Mint (December 2022), available at: https://www.livemint.com/news/india/aiims-computers-information-tech-systems-not-upgraded-for-30-yrs-11670172516721.html, last accessed on May 30, 2023.

4 See: https://www.securityinfowatch.com/cybersecurity/information-security/managed-network-security/article/53012965/the-cybersecurity-implications-of-quantum-computing, last accessed on April 17, 2023.

5 See: https://www.eurofins-cybersecurity.com/news/security-problems-iot-devices/, last accessed on April 17, 2023.

6 See: https://www.techtarget.com/searchsecurity/tip/How-hackers-use-AI-and-machine-learning-to-target-enterprises, last accessed on April 17, 2023.

7 See: https://www.infosecurity-magazine.com/news/chatgpt-creates-polymorphic-malware/, last accessed on April 19, 2023.

8 See: https://www.aicpa-cima.com/news/article/deepfakes-emerge-as-real-cybersecurity-threat, last accessed on May 04, 2023.

Types of Cybersecurity Threats and Liabilities

A. Types of Bad Actors

Cybersecurity threats can arise either from amateur bad actors, or from professionals and organized groups (including states or terrorist organisations). The purposes could range from sheer fun (in case of amateur bad actors) to warfare.

For example, in 2008, an Indian teenager learnt how to hack and access CVV numbers and personal details of people available across various online databases. The teenager worked with a group of people to use these CVV numbers and bank account details to make unauthorised big-ticket purchases.[1] An example of state warfare is the recent reports suggesting that Russian forces were behind the shutdown of the Ukraine's Central Election Commission's computer systems days before the 2014 Ukraine elections.[2]

The threats may be targeted specifically to a group of individuals or organisations, or may be a general threat to all users of a particular website. For example, certain whaling attacks were made against high-ranked executives only, such as employees of Snapchat, Seagate and FACC.[3] User records including personal information and passwords of BigBasket, an online grocery platform, was leaked in 2019. Email IDs and passwords of over 22 million users of Unacademy (one of India's largest online education platforms) was leaked and put up for sale in 2020.[4]

B. Kinds of Threats

The three main kinds of threats are:

i. External threats: these are by external actors, i.e., outside an organisation or entity,

ii. Internal lapses / unauthorized access: this is by actors from within an organisation that might exploit the organisation's system in an unauthorised manner.

iii. Physical security: in relation to compromise of physical locations of computer networks of the company, including due to natural disasters, theft and terrorism.

We have explained these in detail below.

1 See: https://timesofindia.indiatimes.com/city/ahmedabad/big-bucks-drew-kid-hacker-into-cyber-crime/articleshow/3132064.cms, last accessed on May 17, 2023.

2 See: https://www.nbcnews.com/mach/technology/election-cyberattacks-pro-russia-hackers-have-been-accused-past-n673246, last accessed on April 25, 2023.

3 See: https://www.upguard.com/blog/whaling-attack, last accessed on April 25, 2023.

4 See: https://www.business-standard.com/article/companies/unacademy-s-database-hacked-information-of-11-million-users-compromised-120050701280_1.html, last accessed on April 25, 2023.

External Attacks

These are attacks perpetrated by external actors and can have a variety of objectives (such as monetary gains, nuisance, espionage and cyber warfare, etc.). There are several methods which such actors use to externally gain access to computer systems, networks or other infrastructure. Cybercriminals can gain access and remain in a system unnoticed and extracting information for months on end.[5] The top cybersecurity firms' repertoires are based on dealing with these kinds of issues and prevent such attacks in whatever form they come in.

A few examples of such threats are as follows:

- **Malware**: This is intrusive software which is created to gain unauthorised access and eventually lead to leak / breach of confidential information or damage to the system's integrity, among other things.[6] Some examples of malware are ransomware, viruses, worms, spyware, trojan horses. A recent example of malware is the "Emotet" trojan which started in 2014 but erupted again in 2022. This is an advanced trojan malware which is largely spread through phishing emails. Once attachments in an email are clicked, it launches an attack on the user's system to gain access to sensitive information. The spread of this virus was first noticed by the Cybersecurity and Infrastructure Security Agency in the United States and it also saw the virus spread to other countries like France, Japan and New Zealand.[7] This cyber threat is still prevalent as of 2022.[8]

- **Ransomware**: Ransomware is a type of malware that locks users out of their systems and gains access to their sensitive data. It then demands a ransom payment for users to regain access to their systems. A recent example of ransomware is the "Royal ransomware" virus, that India's CERT-In issued a warning against in May 2023.[9] The virus is reported to attack critical sectors such as communications, healthcare, and education and seeks pay-off in bitcoin for not leaking personal data in public domain.

  In 2022, AIIMS in India was under a ransomware attack for over 10 days, and medical records of millions of patients were compromised.[10] Another example is CovidLock, an application that gained popularity during the peak of COVID-19 pandemic. While this application acted as a coronavirus tracking app, in reality it was a malware that threatened to leak social media accounts and delete the host phone's storage unless the victim paid a ransom. Similar apps such as the COVID19 Tracker sought $100 from users in Bitcoin to be paid to the hackers.[11]

5 ERMProtect team, External vs. internal cybersecurity risks: Know the difference, ERMProtect (2022), available at: https://ermprotect.com/blog/external-vs-internal-cybersecurity-risks-know-difference/, last accessed on May 30, 2023.

6 Cisco Team, What is malware? Cisco (July 2021), available at: https://www.cisco.com/c/en_in/products/security/advanced-malware-protection/what-is-malware.html, last accessed on May 30, 2023.

7 CISA Team, Alert (AA20-280A) on Emotet Malware, Cybersecurity and Infrastructure Security Agency (October 2020), available at: https://www.cisa.gov/uscert/ncas/alerts/aa20-280a, last accessed on May 30, 2023.

8 Everette, C., Back from the dead, Emotet malware returns in 2022, Deep Instinct (August 2022), available at: https://www.deepinstinct.com/blog/emotet-malware-returns-in-2022, last accessed on May 30, 2023.

9 PTI, 'CERT-In issues cyber alert against 'Royal' ransomware that attacks health, education sectors', The Hindu (May 2023) Available at: https://www.thehindu.com/business/cert-in-issues-cyber-alert-against-royal-ransomware-that-attacks-health-education-sectors/article66811312.ece, last accessed on May 4, 2023.

10 Sharma, P., AIIMS computers, Information Tech systems not upgraded for 30 yrs, Mint (December 2022), available at: https://www.livemint.com/news/india/aiims-computers-information-tech-systems-not-upgraded-for-30-yrs-11670172516721.html, last accessed on May 30, 2023.

11 Villas-Boas, A., A fake coronavirus tracking app is actually ransomware that threatens to leak social media accounts and delete a phone's storage unless a victim pays $100 in Bitcoin, Business Insider (March 2020), available at: https://www.businessinsider.com/coronavirus-fake-app-ransomware-malware-bitcoin-android-demands-ransom-domaintools-2020-3?IR=T, last accessed on May 30, 2023.

The link between ransomware and cryptocurrency being employed for ransom payments can be observed upon perusing a report published by Sophos, a Britain-based cybersecurity firm, which states that ransomware was fueled by cryptocurrency in 79% of global cybersecurity attacks.[12]

- **Distributed denial-of-service attacks ("DDoS")**: These are attacks where the threat actor directs a large number of machines to bombard a target service with traffic. Due to this, a network becomes overwhelmed and cannot respond to service requests.[13] This is an issue that has *inter alia* plagued online video game developers, with Ubisoft filing and winning against a company that offered such services.[14]
- **Identity theft, spoofing and phishing attacks**: In these attacks, the perpetrator attempts to gain sensitive information such as banking details through fraudulent emails or web-site links by posing as a legitimate business or person. Identity theft is closely linked with phishing attacks. In India, a common method for these attacks is through SMS and online messaging, whereby the perpetrator usually offers enticing rewards or incentives to the victims. Once a user clicks on a link in such messages, the users are redirected to another website, where sensitive information is collected from them. For example, in the past few years, perpetrators would send messages to victims stating they have won a Kaun Banega Crorepati lottery, claiming to be jointly organized by Reliance Jio.[15]

  In case of identity theft, the actors gain sensitive information such as passwords, ID numbers, credit card numbers and social security numbers and misuse them by acting fraudulently on the victim's name.[16] A famous example is the Nigerian Prince scam, where a scammer poses as a wealthy and powerful person in need of some money and promises a lot more money in return.[17] This scam was still raking in over $700,000 a year as of 2019.[18] A more recent example is when Microsoft warned of spear phishing campaigns undertaken by a Russian hacking group that targeted Ukrainian government agencies and NGOs in February 2022.[19] Indian brands such as Amul have also taken action against fake websites using the Amul brand to dupe businesses and individuals by offering fake dealerships and jobs.[20]
- **Fake mobile phone apps**: These can take form of apps that impersonate legitimate brands and convince users to install a cloned app. Preying on the user's false sense of security, they can steal credentials and intercept SMS authentication codes. For example, 'Update Whatsapp' which was a fake WhatsApp application available on the Google Play Store. This false application replicated WhatsApp and flooded users with adverts. This application reportedly had more than 1 million downloads before being taken off the Play Store.[21]

12 Tech desk, "*Unregulated cryptocurrency fueling ransomware attacks globally*", The Indian Express Times (November 2021), available at https://indianexpress.com/article/technology/crypto/nearly-79-percent-of-cybersecurity-incidents-in-18-months-fueled-by-cryptocurrency-report-7637054/, last accessed on April 6, 2023.

13 Editor, C.S.R.C.C. DDoS - glossary: CSRC, CSRC Content Editor, Computer Security Resource Center, available at: https://csrc.nist.gov/glossary/term/ddos, last accessed on May 30, 2023.

14 Chalk, A., Ubisoft wins $150,000 lawsuit against Rainbow Six Siege Ddos Operation, PC Gamer (July 2021), available at: https://www.pcgamer.com/ubisoft-wins-dollar150000-lawsuit-against-rainbow-six-siege-ddos-operation/, last accessed on May 30, 2023.

15 Delhi Cyber Crime Unit, 'KBC Lottery Fraud', Delhi Police (January 2020), available at: https://cyber.delhipolice.gov.in/KBClottery.html, last accessed on May 4, 2023.

16 ESET Team, Identity theft definition and protection ESET, ESET, available at: https://www.eset.com/in/identity-theft/, last accessed on May 30, 2023.

17 AARP What you need to know about Nigerian prince scams, AARP (2022), available at: https://www.aarp.org/money/scams-fraud/info-2019/nigerian.html#:~:text=You%20get%20an%20unsolicited%20email,of%20the%20sender's%20home%20country., last accessed on May 30, 2023.

18 Leonhardt, M., 'Nigerian prince' email scams still rake in over $700,000 a year-here's how to protect yourself, CNBC (April 2019), available at: https://www.cnbc.com/2019/04/18/nigerian-prince-scams-still-rake-in-over-700000-dollars-a-year.html, last accessed on May 30, 2023.

19 Rosenthal, M., 15 examples of real social engineering attacks - updated 2022, Tessian. (February 2022), available at: https://www.tessian.com/blog/examples-of-social-engineering-attacks/, last accessed on May 30, 2023.

20 R. Bhishan, "Amul gets legal relief; court restrains fake websites from using the Amul name", The Economic Times (August 2020), available at: https://economictimes.indiatimes.com/industry/cons-products/fmcg/amul-gets-legal-relief-court-restrains-fake-websites-from-using-the-amul-name/articleshow/77821555.cms?from=mdr, last accessed on May 30, 2023.

21 Sulleyman, A. You might have downloaded a fake version of WhatsApp, Independent Digital News and Media (November 2017), available at: https://www.independent.co.uk/tech/whatsapp-app-android-messaging-apps-fake-google-play-a8039806.html, last accessed on May 30, 2023.

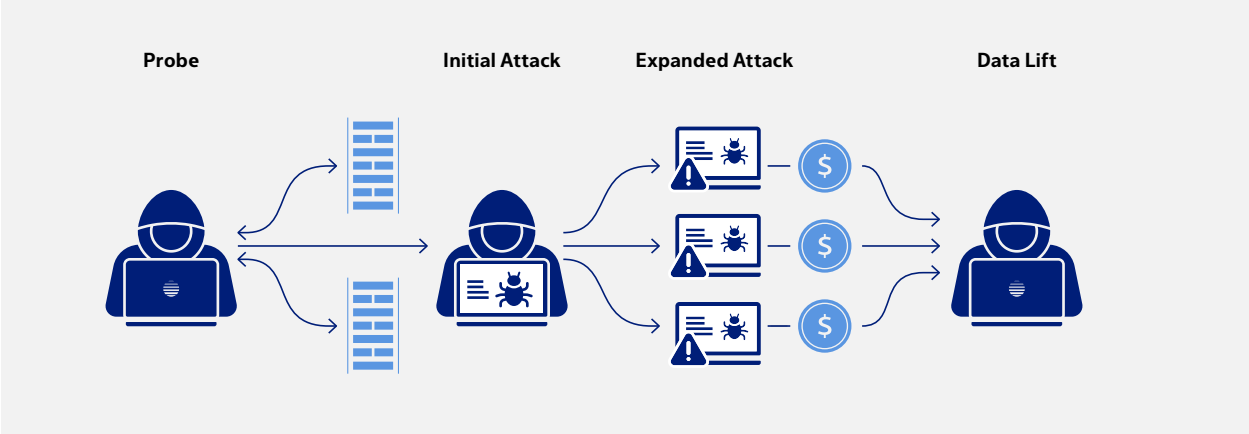
- **SCADA Attacks**: Supervisory control systems ("**SCADA**") are used for monitoring and remotely controlling certain systems including oil and gas pipelines and electrical power transmission and distribution. These kinds of systems are targets since they are often spread across multiple systems and can be made victim to malware.[22]

  An example of such an attack is when cyber criminals hacked into Target's control systems. They were able to access Target's business network and steal credit card information reportedly costing Target $202 million.[23]

- **Attack on Servers**: Server-side attacks are aimed at compromising and breaching data and applications present on a server. These are opposed to client-side attacks which specifically target software present on the desktop. Some examples of vulnerable applications that can be targeted by cyberattacks are server-based applications such as web browsers, media players, email clients, office suites, etc.

- **Data breach / data leak**: A data breach is said to occur when information is stolen from a company without the knowledge of the system owners. This kind of data may include sensitive and proprietary information or confidential information such as credit card numbers, trade secrets or other customer data. An example of such external data breach is when the hotel chain Marriot was hacked and saw about 383 million customer records being subsequently accessed. This breach was allegedly committed by a group of cyber attackers and included passport numbers and payment card details.[24]

How a Data Breach Occurs



Source: DNSstuff[25]

22 SCADA system vulnerabilities to Cyber Attack Electric Energy Online, available at: https://electricenergyonline.com/energy/magazine/181/article/SCADA-System-Vulnerabilities-to-Cyber-Attack.htm, last accessed on May 30, 2023.

23 Zimmerman, G. Target settles HVAC data breach for $18.5 million, fnPrime (May 2017), available at: https://www.facilitiesnet.com/hvac/tip/Target-Settles-HVAC-Data-Breach-for-185-Million--39237, last accessed on May 30, 2023.

24 Glossary, What is Data Breach? How they happen and how to stop them, Abnormal, available at: https://abnormalsecurity.com/glossary/data-breach, last accessed on May 30, 2023.

25 DNSstuff, What is a Data Breach? Ultimate Guide to Cyber Security Breaches, available at: https://www.dnsstuff.com/data-breach-101, last accessed on May 10, 2023.

Internal Lapses / Unauthorized Access

Internal threats in cybersecurity are those which originate from attackers within an organisation that might exploit the organisation's system in an unauthorised fashion, cause damage or commit theft. These can be by negligent employees, malicious insiders, credential thieves, contractors or vendors. Some examples of internal lapses are employee sabotage, accidental or intentional disclosure of data, theft of physical devices, downloading of malicious content and unauthorised devices accessing a private network. These threats pose a different challenge from those posed by outsiders, since the attacker / actor is an insider having easy or ready access. A report by IBM Security conducted by Ponemon Institute[26] stated that incidents of internal threats are rising, with incidents increasing by 47% from 2018 to 2020. The costs of these incidents, i.e. the costs organisations are incurring due to internal threats and events, comprise of costs of surveillance, investigation, incident response, escalation, containment, ex-post response and remediation. The same report stated that the cost of such incidents has increased from 2016 to 2019 from $493,093 to $871,686. If these incidents involve a negligent employee or contractor, each incident can average $307,111 and almost triple in cost if it is an imposter or thief that steals credentials. Some examples of internal threats and their liabilities include:

- **Malicious insiders**: They can act to harm an organisation knowingly, motivated by incentives such as financial gain. This can range anywhere from stealing valuable information and defacing websites to wiping out of entire databases.
- **Employees' negligence**: Employees may at times unintentionally expose their passwords or confidential information to untrusted environments or actors. They can also fall victim to attacks like phishing scams on their work computer, which could gain an outsider access to company information. In a data security incident on major trading platform Robinhood, the perpetrators socially engineered a customer support employee leading to unauthorised access to millions of people's personal information.[27]
- **Moles**: These are people who join a company with the intention to harm them in the future such as by compromising cybersecurity.[28]
- **Data breach/Data leak**: These kinds of threats can even be caused by internal actors. An example of such data breach is when two support staff of the popular e-commerce application Shopify stole customer data from its sellers.[29]

Physical Security

Cybersecurity may also be compromised due to physical factors natural disasters, robberies, theft and terrorism. The types of physical threats can be classified as:

- **Unauthorised access**: A common security risk pertaining to physical systems is the unauthorised access to confidential information. This can come from intruders or hackers. A common form of this kind of threat is known as tailgating, where an unauthorised person follows an authorised person into a secured

26 Ponemon Institute, Ponemon Institute's 2020 Cost of an Insider Breach Report, IBM Security (2021), available at: https://www.ibm.com/security/digital-assets/services/cost-of-insider-threats/#/., last accessed on May 30, 2023.

27 Team Robinhood, Robinhood announces Data Security Incident (update), Robinhood (November 2021), available at: https://blog.robinhood.com/news/2021/11/8/data-security-incident, last accessed on May 30, 2023.

28 Grimmick, R. What is an insider threat? definition and examples, Varonis. (June 2022), available at: https://www.varonis.com/blog/insider-threats, last accessed on May 30, 2023.

29 Whittaker, Z., US charges California man over Shopify Data Breach, TechCrunch (April 2021), available at: https://techcrunch.com/2021/04/05/shopify-breach-hacker-indicted/, last accessed on May 30, 2023.

area. Stealing identification is another way that people who are not a part of an organisation can gain access to a workplace. These kinds of threats highlight the importance of security measures such as access control and surveillance.[30]

- **Intentional acts of destruction**: This refers to acts done by malicious actors wherein deliberate damage is caused to hardware. These acts can be committed by malicious actors conspiring to cause harm to an organisation by damaging information systems such as servers and personal computers. These include theft, arson and vandalism.[31]
- **Disasters** (leading to damage to infrastructure): This can refer to acts wherein damage is unintentionally caused to hardware and other systems. They can be further classified as those caused due to: (i) Human error: These may be in the form of unintentional disastrous acts such as spilling liquids on machines, overloading electrical outlets which may lead to a short circuit occurring and bad plumbing, which may lead to water getting leaked onto important electricity based machines or documents[32]; and (ii) Natural disasters and environmental conditions: These can include the loss of data and hardware from natural events such as floods, fire, storms, earthquakes and lightning strikes. Certain environmental conditions may also affect the working of hardware, software and employees. These can include extreme temperatures, which may affect the office premises, high humidity and heavy rains, which can affect the structure of the building, etc.[33]

C. Liabilities / Risks

i. Data Loss

Data loss, which may be caused by individuals, systems, or actions from within or outside of an organisation, is the intentional or unintentional destruction of information. Loss of data could bring institutions to a standstill, depending on the extent of data loss. For example, the 2011 Georgia hospital incident detailed below in point (iv) led to the temporary shutdown of the non-emergency operations of the hospital. Data loss would also lead to financial and reputation loss for the company, especially when individuals' data collected by the company is lost.

For example, back in 2009, the Microsoft Sidekick servers experienced failure and lost customer data of several customers, including contacts, calendar appointments, and to-do lists. Users lost all the data that was backed up on Sidekick's servers and were not saved on their devices. The company that made the device Sidekick, Danger, did not have proper backup of this data as well, and therefore, the lost data was not recovered.[34]

ii. Financial Risk

Financial cyber risks have become more prominent in recent times, with increased adoption of digital banking and payment methods, especially since the Covid-19 pandemic. Fraudulent financial transactions, extortion, and credit card frauds are the most common types of financial cybersecurity incidents.

30 Ahola, M., Top 5 physical security risks - and how to protect your business, usecure Blog (May, 2021), available at: https://blog.usecure.io/physical-security-risks, last accessed on May 30, 2023.

31 Id.

32 Id.

33 Id.

34 See: https://techcrunch.com/2009/10/10/t-mobile-sidekick-disaster-microsofts-servers-crashed-and-they-dont-have-a-backup/?guccounter=1&guce_referrer=aHR0cHM6Ly9zdHJvbmdob2xkZGF0YS5jb20v&guce_referrer_sig=AQAAAEmKHhrhGlQ3IAc-VHtkxhs_NKta2Q9uvC3PA4KoF03UpNa2mV2k7CmoA7qLytk2zh9gEFn68SepYBVa7X3iq4bsTlOfwH8igpN-B3fal3dNnbnz2adJswIiYxXZfUqX4DHI1xxh0K6wTQbJ3Jhc_WV9SirQIZQsGRgZqnXPDMyp, last accessed on May 30, 2023.

At an individual level, individuals' banking details including digital banking details could be stolen. Institutional level cybersecurity incidents could lead to (i) financial data of customers, vendors, employees and other parties being leaked, (ii) financial loss through unauthorized transactions, and (iii) leaks of sensitive information of institutions that may affect the valuation and share prices of companies, such as unpublished information relating to company performance or financials.

In 2014, JPMorgan Chase, the sixth-largest bank in the world, reported a data breach of over 7 million small businesses and 76 million households in 2014.[35] While the bank released a statement that hackers stole personally identifiable information, including email, phone numbers, names, and postal addresses associated with bank accounts, it denied that passwords were stolen in the breach. Capital One, an American bank, was a victim of data breach in 2019.[36] In the attack, a hacker gained access to over 100 million customers' bank accounts and credit card applications.

Financial risk arising from cybersecurity also exists in non-banking industries, such as cryptocurrency, gaming, and e-commerce applications. Loss of access to cryptocurrency wallets is a common financial risk, as hackers are able to take control of wallets and there are only limited ways for the wallet owner to try to regain access (due to lack of regulatory oversight in several jurisdictions including India). In 2019, about $293 million worth of cryptocurrency and 510,000 user logins were stolen from 12 crypto-exchanges, while 2020 saw nearly $3.78 billion stolen with around $281 million taken in just one attack against the KuCoin exchange.[37]

There are several instances of insiders using their insider access to companies, to steal critical information and divulging it to competing firms for their own financial benefit. Darknet vendor Apostolos Trovias, aka "The Bull," was charged with money laundering and securities fraud in July 2021.[38] By offering securities-related information on AlphaBay, Dream Market, Nightmare Market, and ASAP based on proprietary corporate information (allegedly provided to him by sources within the companies), he undertook insider trading. In particular, pre-release publicly traded corporate earnings reports and trading tips, including single tips, weekly and monthly plans, were sold in return for Bitcoin.

iii. National Security Risk

Countries at large are susceptible to cybersecurity attacks, which in turn may lead to significant risk to national security. In addition to growing dependencies on technology to hold valuable and sensitive information at a national scale, various national-level activities undertaken are increasingly reliant on networks of connected devices. India's AIIMS, in 2022, came under a ransomware attack where medical records of millions of patients were compromised and the hospital had to revert to physical paperwork for managing patients.[39] In 2020-2022, Sri Lanka faced a series of cyberattacks, including on the Google.lk domain, the websites of the health and energy ministries, and certain embassies based in the country.[40]

35 See: https://www.forbes.com/sites/maggiemcgrath/2014/10/02/jp-morgan-says-76-million-households-affected-by-data-breach/?sh=22a5d017a2af, last accessed on May 30, 2023.

36 See: https://www.cnet.com/personal-finance/capital-one-190-million-data-breach-settlement-today-is-deadline-to-file-claim/#:~:text=The%20massive%20cyberattack%20went%20undiscovered,balances%2C%20transactions%20and%20credit%20scores, last accessed on May 30, 2023.

37 See: https://www.techtarget.com/searchsecurity/answer/Is-Bitcoin-safe-The-truth-about-Bitcoin-security-and-crypto-currency, last accessed on May 30, 2023.

38 See: https://www.asisonline.org/security-management-magazine/latest-news/online-exclusives/2022/the-bull-and-millionaire-mike-a-look-at-darknet-and-securities-fraud--summary/, last accessed on May 30, 2023.

39 Sharma, P., AIIMS computers, Information Tech systems not upgraded for 30 yrs, Mint (December 2022), available at: https://www.livemint.com/news/india/aiims-computers-information-tech-systems-not-upgraded-for-30-yrs-11670172516721.html, last accessed on May 30, 2023.

40 See: https://en.wikipedia.org/wiki/2021_cyberattacks_on_Sri_Lanka, last accessed on April 25, 2023.

iv. Infrastructure Risk

Infrastructure risk is in reference to the risks posed to electric grids, telecom networks, and other critical infrastructure dealing with public utility distribution. Infrastructure level attacks have the potential to bring various facets of communication or utilities to a standstill. For example, in 2017, over 60,000 Bharat Sanchar Nigam Limited (**"BSNL")** (one of India's public telecom service providers) broadband modems became dysfunctional after a malware attack[41], and in 2018, BSNL was locked out of its own intranet portals and the portals used to make bill payments by the public.

v. Reputational Risk

Individuals that lose their personal and sensitive information in cyberattacks run the risk of harm to their reputation. This could include personal content that may include compromising information regarding the individual, and individual communication that may cause issues when shared with third parties, such as employers or publicly accessible websites.

Businesses and other institutions may also face reputations risks due to security breaches. A business may sustain severe losses as a result of a cyberattack, and any loss (whether monetary, of information, etc.) could lead to loss of consumer trust in the company. Given that trust is an essential element of a consumer relationship, loss of trust may lead to loss of customers, drop in sales, and reduction in profits. The effect of reputational damage may impact the company's relationships with its suppliers, partners, investors and other third parties interested in the business. Nearly 60% of small businesses affected by a data breach are likely to go out of business due to reputational damage.[42] In larger companies, the reputational cost of a data breach may affect the company's stock prices. In 2018, Meta's stock had fallen by 7%, a $43 billion loss after the data breach incident involving Cambridge Analytica.[43]

vi. Risk to Human Safety

In relation to human safety, cybersecurity in the healthcare, utility services and hazardous industries are relevant. Sensitive information includes patient databases, hospital and treatment center information systems, and laboratory systems and networks. The risks include shutdown of healthcare institutions and services, incorrect services offered, and lack of data to provide effective healthcare, amongst other risks.

In December 2011, a hospital in Georgia, USA, was forced to divert all non-emergency admissions to other medical centers after a malware attack brought down the institution's IT network, and required staff to use paper records. The attack affected computer connectivity as hospitals could not communicate with each other. The hospital was forced to use a runner system, where papers were shuttled by personnel from station to station.

Medical device tampering, phishing (which targets doctors' email addresses), and denial of service attacks are some examples of harmful activities that could specifically affect healthcare organisations. Hackers attacked the databases of SingHealth, the largest healthcare provider group in Singapore, which ultimately resulted in the loss of personal information of 1.5 million patients.[44]

41 See: https://www.thehindu.com/news/national/karnataka/malware-affects-thousands-of-bsnl-broadband-modems/article19381410.ece, last accessed on April 25, 2023.

42 See: https://www.inc.com/joe-galvin/60-percent-of-small-businesses-fold-within-6-months-of-a-cyber-attack-heres-how-to-protect-yourself.html, last accessed on May 30, 2023.

43 See: https://www.theverge.com/2018/3/19/17139642/facebook-stock-fall-market-cap-data-breach-cambridge-analytica, last accessed on May 30, 2023.

44 See: https://graphics.straitstimes.com/STI/STIMEDIA/Interactives/2018/07/sg-cyber-breach/index.html, last accessed on May 30, 2023.

vii. Business Risks[45]

Cybersecurity threats and past cybersecurity incidents may lead to hurdles at the time of seeking investments. Typically, questions posed at the time of due diligence relate to the types of data that a company collects from individuals, whether the company is in adherence with security measures required under law, if the company shares such data with other companies or third parties, and if the company has put in place the required measures for reporting of cybersecurity incidents. These questions are asked to understand the robustness of the systems currently employed by companies, and to understand the extent of the company's past cybersecurity incidents.

Lack of sufficient security measures, and past cybersecurity incidents may lead to loss of confidence of investors. The consequences of having a less than robust cybersecurity policy and any past cybersecurity incidents may lead to: investors devaluing the investment in the company, investors requiring specific representations and warranties and indemnities from the company, investors choosing not to invest in the company, regulators adding additional conditions to any approvals provided to the company, and/or regulators refusing approvals to the company.

45 See: https://www.nishithdesai.com/SectionCategory/33/Research-and-Articles/12/60/NDAHotline/6175/1.html, last accessed on May 30, 2023.

Comparison of Cybersecurity Framework in Various Jurisdictions

Before coming to the regulatory framework on cybersecurity in India, it is pertinent to review in brief the applicable framework in some of the prominent jurisdictions.

A. US[1]

In the US, numerous federal and state laws contain cybersecurity requirements. US federal cybersecurity laws currently apply to specific industries or types of data; at present there is no universally applicable federal cyber law. For example, there are requirements applicable to medical device manufacturers,[2] financial institutions,[3] electric utilities,[4] and airport and aircraft operators;[5] as well as organizations handling certain health information[6] or export-controlled data.[7] There are also a number of cybersecurity requirements applicable to entities contracting with the federal government. New requirements for cybersecurity governance, risk management, and incident reporting are expected shortly for publicly traded companies and others registered with the Securities and Exchange Commission ("**SEC**").[8] Many of the cybersecurity laws that apply to specific industries or types of data have reporting/notification requirements that stretch from mere hours for certain highly regulated sectors, up to 60 days. In some cases, those requirements apply to security incidents, even if they do not give rise to a data breach, but in most cases, notice is only required if specific types of data are accessed without authorization. A new law will require cyber incident and ransom payment reporting for certain critical infrastructure entities, once implementing regulations are proposed and finalized.[9]

At the state level, various laws and regulations include cybersecurity requirements. Those laws often rely on a standard of "reasonable security," although in some cases they impose detailed requirements. For example, the New York SHIELD Act[10] and Massachusetts Data Security Regulations[11] both impose specific requirements for cybersecurity programs and safeguards, tied to the scope of protecting personal data of those states' residents. In addition, US states and territories each have adopted breach notification laws, with varying requirements and triggers; reporting timeframes range from days to a month or more, with some of the laws not specifying a timeframe (although generally clarifying that notice should occur without unreasonable delay).

1 Contributed by Nathan Salminen (Counsel) and Paul Otto (Partner), Global Regulatory Group, Hogan Lovells, Washington DC.

2 See, e.g., https://www.fda.gov/medical-devices/digital-health-center-excellence/cybersecurity.

3 See, e.g., https://www.ftc.gov/business-guidance/privacy-security/gramm-leach-bliley-act.

4 See, e.g., https://www.ferc.gov/industries-data/electric/industry-activities/cyber-and-grid-security.

5 See, e.g., https://www.tsa.gov/news/press/releases/2023/03/07/tsa-issues-new-cybersecurity-requirements-airport-and-aircraft.

6 See, e.g., 45 C.F.R. Part 164, Subpart C.

7 See, e.g., 22 C.F.R. Parts 120–30.

8 See, e.g., https://www.sec.gov/news/press-release/2022-39 (publicly traded companies); https://www.sec.gov/news/press-release/2023-52 (broker-dealers and others.

9 See: Cyber Incident Reporting for Critical Infrastructure Act of 2022 ("**CIRCIA**"); https://www.cisa.gov/topics/cyber-threats-and-advisories/information-sharing/cyber-incident-reporting-critical-infrastructure-act-2022-circia.

10 See: N.Y. Gen. Bus. Law § 899-bb.

11 See: 201 CMR 17.00 et seq.

The various cybersecurity and breach notification laws in the US are enforced by different entities. For example, the Cybersecurity and Infrastructure Security Agency (**"CISA"**) is the national agency responsible for understanding, managing, and reducing risk to US cyber and physical infrastructure.[12] CISA is tasked with protecting US critical infrastructure and encourages entities owning and/or operating critical infrastructure to voluntarily share information on cyber incidents with CISA. For another example, the Federal Trade Commission (**"FTC"**) has brought numerous enforcement actions against companies that it alleges failed to implement reasonable security measures.[13] In initiating these actions, FTC has derived authority from Section 5 of the FTC Act relating to unfair and deceptive trade practices.[14] At the state level, various Attorneys General and other state agencies have cybersecurity regulatory authority.

B. United Kingdom[15]

The UK does not have an overarching national law that deals exclusively with cybersecurity. Instead, there are several legislative instruments that make up the cybersecurity legal framework. Some of these instruments apply more generally across sectors, such as the UK GDPR,[16] whereas others are sector-specific such as the Telecommunications (Security) Act[17] and the Medical Devices Regulation.[18]

The UK GDPR and Data Protection Act[19] apply to organisations that process personal data. These laws require organisations to have in place appropriate security measures to prevent personal data from being accidentally lost, destroyed or damaged. The UK GDPR does not prescribe the security measures to be implemented. Instead, it requires organisations to assess the 'appropriate' level of security based on factors including the risks presented by the processing, the state of the art in security measures and the cost of such measures. Where there is a personal data breach, the UK GDPR requires organisations to report certain breaches to the data protection authority (ICO) within 72 hours of becoming aware of the breach. Failure to notify the ICO when required can result in a fine of up to £8.7 million or 2% of the organisation's global turnover, whichever is higher. In relation to failure to meet the data security obligations themselves, and other contraventions, the ICO has the power to impose fines of up £17.5 million or 4% of the organisation's global turnover, whichever is higher.

PECR[20] sits alongside the UK GDPR and the Data Protection Act. PECR requires that service providers (such as telecoms providers or internet service providers) take appropriate technical and organisational measures to protect the security of that service. Although the factors to be considered are different to the UK GDPR, the overall approach as to what constitutes 'appropriate' measures, is similar. Where there is a breach of PECR, the ICO has the power to take action against the organisation, including criminal prosecution, non-criminal enforcement such as a monetary penalty, and audit. A monetary penalty of up to £500,000 can be issued against the organisation or its directors. The new Data Protection and Digital Information Bill[21] seeks to increase maximum fines so as to bring them into line with current monetary penalties under the UK GDPR.

12 See: https://www.cisa.gov.

13 See: https://www.ftc.gov/datasecurity.

14 Id.

15 Contributed by Tarryn Smith (Associate) and Marc Dautlich (Partner), Bristows LLP, London.

16 The retained EU law version of the General Data Protection Regulation ((EU) 2016/679.

17 Telecommunications (Security) Act 2021.

18 Medical Devices Regulations 2002.

19 Data Protection Act 2018.

20 The Privacy and Electronic Communications (EC Directive) Regulations 2003.

21 Data Protection and Digital Information (No. 2) Bill [Bill 265 2022-23].

The NIS Regulations,[22] which, at the date of writing, are also in the process of being updated, are aimed at improving the security and continuity of critical infrastructure and essential services that rely on network and information systems. The NIS Regulations apply to operators of 'essential services' as well as relevant 'digital service providers', essentially operators of so-called 'critical national infrastructure'. The NIS Regulations require organisations to comply with security requirements to protect against risks to and minimise incidents in respect of network and information systems used to provide their services, and to notify regulators of certain incidents that impact those services. A range of different regulators, depending on the affected industry in question, can take action to enforce NIS. Each has powers to issue enforcement notices and financial penalties, and powers of inspection. In serious cases, competent authorities can issue monetary fines of up to £17 million (which unlike the UK GDPR are tiered and based on the materiality and effect of the non-compliance).

The Computer Misuse Act[23] is the principal legislation that criminalises unauthorised access to, or modification of, a 'computer system' or data. A review of the Act in May 2021 to assess potential legislative updates was followed by a consultation in February 2023, seeking views on three main proposals, including domain name and IP address takedown and seizure powers, power to preserve data, and creating a general offence for possessing or using illegally obtained data. These proposals would give law enforcement bodies greater powers in cyber investigations. The consultation remains underway at the time of writing.

C. Germany[24]

There are several laws applicable to cybersecurity in Germany, with the most significant being the Act on the Federal Office for Information Security ("**BSIG**"), which lays out the basic obligations in relation to cybersecurity. Notably, there are additional laws providing cybersecurity regulations to specific sectors such as banking and insurance, telecommunications and securities.

The BSIG, first of all, applies to operators of critical infrastructure. The related Ordinance for the Designation of Critical Infrastructures ("BSI-KritisV") defines which entities are considered critical infrastructures in the context of the BSIG. The BSI-KritisV determines the relevant categories of potential critical infrastructure (e.g., health care, finance or communications) and thresholds for the applicability of the BSIG, mostly connected to size, turnover, etc.) Secondly, the BSIG also applies to digital service providers. Digital service providers (not already being covered as critical infrastructure) are subject to the BSIG based on their company size i.e. if the digital service provider is at least considered as a medium-sized enterprise, i.e. an enterprise which (i) employs 50 or more persons and/or (ii) whose annual turnover and/or annual balance sheet total does exceed EUR 10 million.

Companies subject to BSIG must take appropriate organizational and technical measures to manage risks and prevent disruptions to the availability, integrity, authenticity and confidentiality of their systems.[25] Operators of critical infrastructure have to prove compliance with these measures to the Federal Office for Information Security ("**BSI**") on a regular basis.[26]

22 Network and Information Systems Regulations 2018.

23 Computer Misuse Act 1990.

24 Contributed by Christian Saßenbach (Associate) and Dr. Jürgen Hartung (Partner), Oppenhoff, Cologne.

25 Section 8a(1) and 8c(1) of BSIG.

26 Section 8a(3) of BSIG.

Furthermore, in case of failure or significant impairment of functionality, Operators of critical infrastructure must report disturbances in the availability, integrity, authenticity, and confidentiality of their IT systems, components or processes to the BSI without undue delay. The report must contain information on the disruption, possible cross-border effects and technical framework conditions. According to the BSIG, a reporting obligation even results from the mere possibility of a failure or impairment if the disruption is significant.[27] In this respect, German legislation currently goes beyond the requirements of the NIS-Directive.

Digital service providers are subject to a similar reporting obligation in case of any cybersecurity incident that has a significant impact on the provision of their service.[28]

In the event of violations, the BSI can demand the necessary measures for elimination, but can also impose administrative fines. The amount of the respective administrative fine depends on the specific violation, but can be up to EUR 20,000,000.

D. Singapore

The Cybersecurity Act 2018[29] of Singapore was enacted to prevent, manage and respond to cybersecurity threats and incidents.[30] Under the Act, the Commissioner of Cybersecurity is empowered to designate computers or computer systems as "Critical Information Infrastructures" ("**CII**") if they are located wholly or partly in Singapore and if they are necessary for the continuous delivery of essential services like national security, defense, foreign relations, economy, public health, safety and order.[31]

CIIs must report the occurrence of cybersecurity incidents to the Commissioner within a fixed period of time in a specific form, else be liable to a fine of up to SGD 100,000 or imprisonment not exceeding 2 years or both.[32] The Cybersecurity (Critical Information Infrastructure Regulations) 2018 ("**Cybersecurity Regulations**") stipulate that a CII owner must report the Commissioner of a cybersecurity incident within two hours of its occurrence with details regarding the affected CII, its owner, the nature of the incident and when and how it occurred, the resulting effect and the details of the person reporting the incident.[33] In addition, the CII owner is required to provide supplementary information pertaining to the cause, impact and measures taken, within a span of 14 days.[34]

The Personal Data Protection Act 2012 also requires organizations to conduct an assessment of 'notifiable data breaches'[35] and thereafter notify such occurrence to its Data Protection Commission in a manner that is as soon as practicable but no later than 3 days since the assessment.[36]

27 Section 8b(4) of BSIG.

28 Section 8c(3) of BSIG.

29 Available at: https://sso.agc.gov.sg/Act/PDPA2012?ProvIds=P16A-#pr26B-, last accessed on May 30, 2023.

30 Preamble of the Cybersecurity Act, 2018.

31 Section 7 read with Section 2(1) of the Cybersecurity Act, 2018.

32 Section 14 of the Cybersecurity Act, 2018.

33 Regulation 5 of the Cybersecurity Regulations.

34 Regulation 5 of the Cybersecurity Regulations.

35 As per Section 26B of the Personal Data Protection Act 2012, a data breach is a notifiable data breach if the data breach — (a) results in, or is likely to result in, significant harm to an affected individual; or (b) is, or is likely to be, of a significant scale.

36 Section 26C & Section 26D of the Personal Data Protection Act 2012.

Regulatory Framework in India

A. National Cyber Security Policy, 2013

India's National Cyber Security Policy dates back to 2013 and was created with the vision of building "*a secure and resilient cyberspace for citizens, businesses and Government*".[1] The policy recognized the threats that cyberattacks carry, and the potential risks to human lives, the economy, and national security. The policy also identified key strategies for securing the cyberspace, most of which are applicable today. However, given that the policy is a decade old, a revised national policy for cybersecurity is well overdue. The Government had stated in December 2022 that it had formulated a draft cybersecurity strategy pertaining to the security of national cyberspace.[2] However, the details of the strategy and timelines for implementation were not mentioned.

B. Cybercrimes Recognized under Indian Law

I. Information Technology Act, 2000 ("IT Act")

The IT Act provides, *inter alia*, for punishment for offences committed relating to electronic communication or data, and other offences in relation cybersecurity. Certain offences such as access to computers, computer systems or computer networks without the permission of the owner/person in charge, downloading or copying data from computers, and denial of access to computers also make the perpetrator liable to pay compensation.

Some of these offences are detailed below:

- **Computed related offences**

  Section 43 of the IT Act provides for compensation payable for certain actions in relation to computer infrastructure (i.e., computer, computer system, computer network) and computer resources when taken without the owner or person in charge of such computer infrastructure or resource. This includes unauthorized access, downloads, introduction of computer contaminants, damage, denial of access, among other acts. Under Section 66, these actions if done dishonestly or fraudulently, are punishable with imprisonment up to 3 years, and / or a fine up to INR 500,000. Further, if any person has secured access to material containing personal information about another person, and discloses the same without the consent of the person, with the intent to cause or knowing that he is likely wrongful loss or wrongful gain, is punishable with imprisonment up to 3 years, and / or a fine up to INR 500,000.[3]

1 See: https://www.meity.gov.in/writereaddata/files/downloads/National_cyber_security_policy-2013%281%29.pdf#:~:text=To%20protect%20information%20and%20information,%2C%20processes%2C%20technology%20and%20cooperation, last accessed on May 30, 2023.

2 See: https://www.thehindu.com/news/national/national-security-council-secretariat-formulated-draft-national-cyber-security-strategy-centre/article66262515.ece, last accessed on May 30, 2023.

3 Section 72A of the IT Act; Section 23 of the IPC defines "Wrongful gain" as 'gain by unlawful means of property to which the person gaining is not legally entitled.', and "Wrongful loss" as 'the loss by unlawful means of property to which the person losing it is legally entitled.'

- **Tampering with computer source documents**

  The intentional concealment, destruction or alteration of computer source code when such source code is required to be kept or maintained under any applicable law is punishable with imprisonment of up to 3 years and/or with fine of up to INR 200,000[4]

- **Dishonestly keeping stolen device/resource**[5]

  A person who dishonestly keeps or receives any stolen electronic resource, knowing that such resource or device is stolen, may be punished with imprisonment of up to 3 years, and/or a fine of up to INR 100,000.

- **Identity theft**[6]

  Identity theft involves fraudulent or dishonest use by a person of electronic signature, password or any other unique identification feature of another person. It is punishable with imprisonment up to 3 years, and a fine up to INR 500,000.

- **Impersonation using a computer resource**[7]

  Cheating by means of impersonating a person using a computer resource or electronic device is punishable with imprisonment up to 3 years, and a fine up to INR 100,000.

- **Cyber terrorism**[8]

  Certain acts (such as denial of access to computer resource or unauthorized access) when committed with the intent to threaten the unity, integrity, security or sovereignty of India or to strike terror in people may be categorized as cyber terrorism. Cyber terrorism also includes unauthorized access to any data or information obtained with reasons to believe that such data or information may be used to cause or likely to cause injury to the interests of the sovereignty and integrity of India, the security of the State, friendly relations with foreign States, public order, decency or morality, contempt of court, defamation or incitement to an offence, or to the advantage of any foreign nation, group of individuals or otherwise. Hence, the scope of cyber terrorism is fairly broad, and is punishable with life imprisonment.

The IT Act provides that any of the above criminal offences should be investigated by a police officer not below the rank of an Inspector.[9]

4 Section 65 of the IT Act.
5 Section 66B of the IT Act.
6 Section 66C of the IT Act.
7 Section 66D of the IT Act.
8 Section 66F of the IT Act.
9 Section 78 of the IT Act.

II. Indian Penal Code

While there are specific offences detailed in the IT Act, a person can also take recourse under the general criminal law of India under certain provisions. There are various provisions of the IPC that may include cybercrimes as an offence:

- **Cheating**[10]

  The offence of cheating includes deceiving someone to deliver a property to a person, which he would not have delivered ordinarily if not deceived. In relation to a cyber offence, this could include deceiving someone to send across restricted or confidential data to a person not authorized to receive it, which the person so deceived would have ordinarily known and not sent.

- **Forgery of electronic records**[11]

  This provision makes specific reference to an act with respect to any electronic document, making it a cybercrime. It includes making a false document or electronic record that would either cause damage to another person, or even leading to a false claim on a property. If done with the wrongful intention of committing such an act, it would be said to be forgery, punished with up to 2 years of imprisonment.

- **Receiving stolen property**[12]

  Similar to the IT Act offence, if a person intentionally receives/keeps a stolen property (say on electronic device) knowing it to be stolen, may be punished up to 3 years of imprisonment.

  However, it is a settled position that a special law (in this case, the IT Act) prevails over a general law (i.e., IPC).[13] Hence, if the offence committed is covered under the IT Act as well as the IPC, a charge for commission of such offence can only be made out under the IT Act.

III. Procedure for Reporting and Prosecution of Cybercrime

There are two primary ways in which such complaints can be made:

A. Report to a Police Station

A person can register a complaint with the relevant police station, providing the information relating to the offence committed. Depending on the nature of the offence (cognizable or non-cognizable), the police will either reduce the information in the form of a First Information report ("**FIR**")[14] or refer the person to the magistrate after recording such information.[15] After this, the police commences the investigation (or is directed to investigate by the magistrate[16]) relating to the offence, consequent to which, a criminal proceeding ensues when the magistrate feels there is sufficient reason to proceed.[17]

10 Section 415 of the Indian Penal Code.

11 Section 463 of the Indian Penal Code.

12 Section 411 of the Indian Penal Code.

13 Sharat Babu Digumarti v. Govt Of Nct Of Delhi, Criminal Appeal No. 1222 of 2016 (arising out of S.L.P. (Criminal) No. 7675 of 2015).

14 Section 154 of the CrPC.

15 Section 155 of the CrPC.

16 Section 202 of the CrPC.

17 Section 204 of the CrPC.

B. Register Complaint with National Cyber Crime Reporting Portal

Cybercrimes can be reported only through the National Cyber Crime Reporting Portal.[18] As mentioned above in Section 3(B)(i), this portal is an initiative of the Indian government to facilitate complainants/ victims to report cybercrime complaints online. It provides two options for reporting cybercrimes on the portal: (1) Report Crime related to Women/ Child or (2) Report Other Cybercrimes. Other cybercrimes would include the offences relating to cybersecurity such as online financial frauds, ransomware, hacking, cryptocurrency crimes and online cyber trafficking as detailed in this section above.

While all Indian citizens can report cybercrimes through this portal, the FAQs also state that a complaint can be filed by a person who is *not* an Indian citizen but has been victimized online by an individual or a company in India.[19] Presently, over 30 cities in India have a cyber cell of their own, and the other towns and villages in the state have a separate dedicated cyber cell.[20]

18 See: https://cybercrime.gov.in/, last accessed on May 30, 2023.

19 See: https://cybercrime.gov.in/Webform/FAQ.aspx, last accessed on April 25, 2023.

20 See: https://cybercrime.gov.in/webform/Crime_NodalGrivanceList.aspx, last accessed on April 25, 2023.

C. Indian Computer Emergency Response Team

CERT-In is the national agency of India established under the Information Technology Act, 2000 (**"IT Act"**) for performing various functions with respect to cybersecurity in India, including for:

- collection, analysis and dissemination of information on cyber incidents;
- issuing forecast and alerts of cybersecurity incidents;
- undertaking emergency measures for handling cybersecurity incidents, etc.[21]

CERT-In also has the power to call for information and give directions to service providers, intermediaries, data centers, body corporate and any other person.[22]

The Information Technology (The Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rules, 2013 (**"CERT-In Rules"**)[23] contain certain obligations and responsibilities of CERT-In with respect to cybersecurity incidents (such as response, prediction and prevention, analysis and forensics, etc.).

Importantly, the CERT-In Rules also contain the following requirements with respect to various kinds of entities:

- **Incident reporting**: All individuals, organisations and corporate entities are mandatorily required to report certain identified cybersecurity incidents[24] to CERT-In, as early as possible. Other cybersecurity incidents may be voluntarily reported to CERT-In.
- **Appointment of Point of Contact**: All service providers, intermediaries, data centers and body corporate are required to designate a Point of Contact (**"PoC"**) to interface with CERT-In, and furnish information relating to such PoC to CERT-In in the specified format.
- **Compliance with CERT-In directions and requests for information**: All service providers, intermediaries, data centres, body corporate and other persons are required to provide such information and comply with directions as may be required by CERT-In.

Contravention of the above provisions under the CERT-In Rules may attract liability for compensation (payable to the person affected by such contravention) / a penalty of up to INR 25,000 (approx. USD 320).[25]

---

21 Section 70B of the IT Act.

22 Section 70B(6) of the IT Act.

23 Our analysis of the CERT-In Rules is available at https://www.natlawreview.com/article/reporting-cybersecurity-breaches-india-it-time-to-overhaul-law.

24 The Annexure to the CERT-In Rules identifies the following incidents to be mandatorily reported:

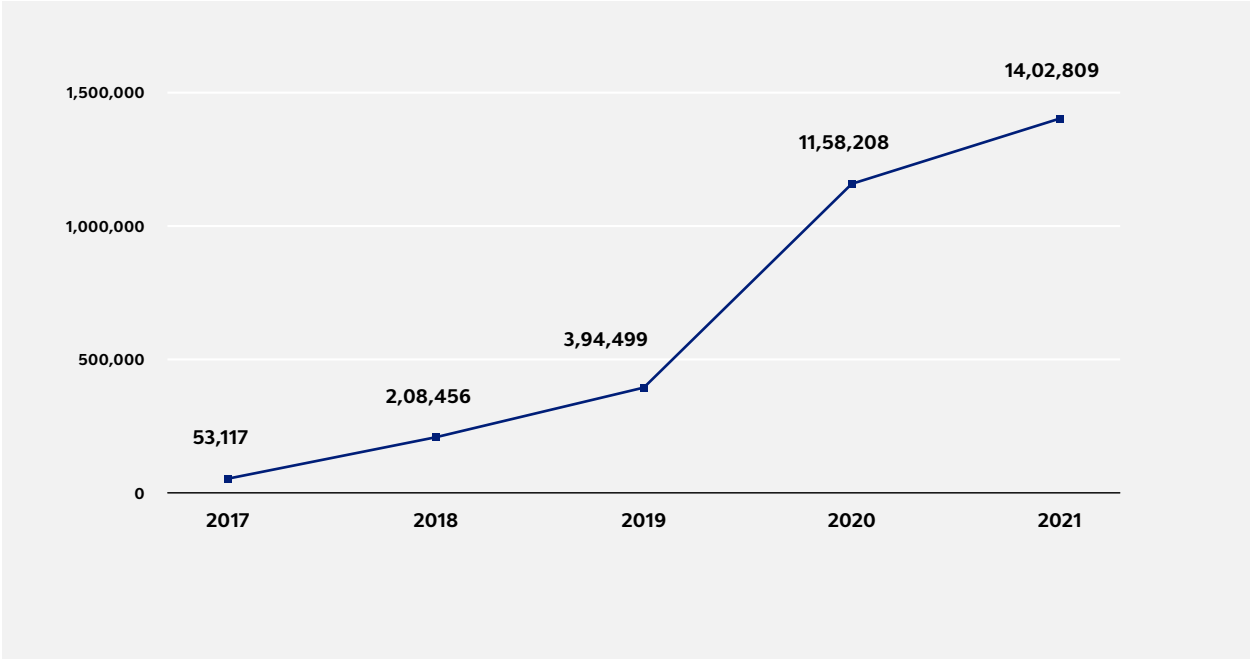
- Targeted scanning/probing of critical networks/systems
- Compromise of critical systems/information
- Unauthorised access of IT systems/data
- Defacement of website or intrusion into a website and unauthorised changes such as inserting malicious code, links to external websites etc.
- Malicious code attacks such as spreading of virus/worm/Trojan/Botnets/Spyware
- Attacks on servers such as Database, Mail and DNS and network devices such as Routers
- Identity Theft, spoofing and phishing attacks
- Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks
- Attacks on Critical infrastructure, SCADA Systems and Wireless networks
- Attacks on Applications such as E-Governance, E-Commerce etc.

25 Section 45 of the IT Act. However, please note that the Directions also contain some requirements which overlap with those under the CERT-In Rules, and non-compliance with the Directions entails a stricter punishment, as specified later.

Subsequently, CERT-In also issued certain directions on April 28, 2022[26] ("**Directions**"), which supplement the CERT-In Rules and contain additional compliance requirements for service providers, intermediaries, data centres, body corporate and Government organisations ("**Entities**"). The Ministry of Electronics and Information Technology ("**MeitY**"), on May 18, 2022, also issued a list of frequently asked questions[27] ("**FAQs**") on the Directions which provide clarifications on certain aspects of the Directions.

Cybersecurity Incidents in India

CERT-IN data indicates a surge in cyberattacks since 2017



Source: The Print[28]

Compliance Requirements under Directions and CERT-In Rules

The Directions and CERT-In Rules, read together, contain some mandatory ongoing compliances and certain conditional compliances which would need to be adhered to by Entities (provided they satisfy the applicability criteria specified below).

26 See: https://www.cert-in.org.in/PDF/CERT-In_Directions_70B_28.04.2022.pdf, last accessed on May 30, 2023.

27 See: https://www.cert-in.org.in/PDF/FAQs_on_CyberSecurityDirections_May2022.pdf, last accessed on May 30, 2023.

28 The Print, India's had its worst year of cyberattacks, but 2023 will See: govt & firms ramp up defences, available at: https://theprint.in/india/indias-had-its-worst-year-of-cyberattacks-but-2023-will-see-govt-firms-ramp-up-defences/1286441/, last accessed on May 10, 2023.

A. Mandatory Ongoing Compliances for Entities

i. Designation of PoC[29]

Entities must designate a PoC to interface with CERT-In. While this requirement was present in the CERT-In Rules as well, the Directions also require the information relating to a PoC to be sent to CERT-In in the format specified in Annexure II to the Directions and updated from time to time.

Notably, there is no requirement for the PoC to be an Indian resident under the Directions or CERT-In Rules. While the PoC may be situated anywhere, CERT-In's expectation would be that such person is approachable as and when they reach out to the PoC.

ii. Maintenance of Logs[30]

Entities must mandatorily enable logs of all its information and communications technology (**"ICT"**) systems and maintain them securely for a rolling period of 180 days. These should be provided to CERT-In along with reporting of any incident or when ordered / directed by CERT-In.

The logs that should be maintained depend on the sector that the Entity operates in, and may include firewall logs, intrusion prevention systems logs, SIEM logs, web / database/ mail / FTP / proxy server logs, event logs of critical systems, application logs, ATM switch logs, SSH logs, VPN logs, etc. This list of logs is not exhaustive but has been mentioned under the FAQs to provide a flavour of logs that should be maintained by the relevant entity. From the incident response and analysis perspective, both successful as well as unsuccessful events have to be recorded.

Logs need not be stored in India so long as the obligation to produce logs to CERT-In is adhered to by the Entity.

iii. System Clock Synchronisation[31]

Entities are required to connect to the Network Time Protocol (NTP) Server of National Informatics Centre (NIC) or National Physical Laboratory (NPL) or with NTP servers traceable to these NTP servers, for synchronisation of all their ICT systems clocks. In case the entity has ICT infrastructure spanning multiple geographies, it can use accurate and standard time source other than NPL and NIC, however, it must ensure that its time source does not deviate from NPL and NIC.

It is not mandatory to synchronise all ICT system clocks with the NPL and NIC servers, or in Indian Standard Time (IST). If there is any deviation between the system clocks of an Entity and the NPL and NIC servers, the Entity should maintain a record of such deviation and provide such information regarding the deviation to CERT-In at the time of reporting an incident.

B. Conditional Compliances for Entities

i. Mandatory Reporting of Incidents[32]

What to report and when: The list of cybersecurity incidents under Annexure I to the Directions (listed in Annexure A) must be mandatorily reported by applicable Entities.[33] Only incidents that are

29 Paragraph (iii) of the Directions.

30 Paragraph (iv) of the Directions.

31 Paragraph (i) of the Directions.

32 Paragraph (ii) of the Directions.

33 Please note that the Directions have added 10 types of incidents to the list of incidents under the Annexure to the CERT-In Rules.

listed in Annexure A and fall within the definition of "cyber security incidents"[34] as defined under the CERT-In Rules are required to be reported to CERT-In as early as possible, as stated in the CERT-In Rules. Further, only confirmed incidents need to be reported.

Additionally, any incident as stated in Annexure A and meeting the following criteria should be reported within 6 hours of the relevant entity having noticed or having been brought to notice of such incident ("**Identified Incidents**"):

- cyber incidents[35] and cybersecurity incidents of severe nature (such as denial of service, distributed denial of service, intrusion, spread of computer contaminant including Ransomware) on any part of the public information infrastructure including backbone network infrastructure;
- data breaches or data leaks;
- large-scale or most frequent incidents such as intrusion into computer resource, websites etc.;
- cyber incidents impacting safety of human beings.

Information to be provided: For Identified Incidents, the Entity may provide information to the extent available within the 6-hour timeline. Additional information may be reported later within a reasonable time to CERT-In. General guidance on the types of information which could be relevant to the incident is provided on CERT-In's website.[36]

Who should report: In case of multiple parties being affected by a cybersecurity incident (such as in case of a third-party service provider's system being affected which also impacts an Entity), the Entity which notices the incident, is required to report to CERT-In. The obligation of reporting of the incident is neither transferrable nor can it be indemnified against or dispense with. Nevertheless, in practice, the Entity which owns / has control over the Computer Infrastructure (defined below) which has been impacted will be required to report.

Reporting format: The incidents can be reported to CERT-In via email (**incident@cert-in.org.in**), Phone (1800-11-4949) and Fax (1800-11-6969). The details regarding methods and formats of reporting cybersecurity incidents is also published on the website of CERT-In (**www.cert-in.org.in**).

ii. Compliance with CERT-In Directions and Provision of Information / Assistance

When CERT-In issues any order/directions to any Entity, such entity must mandatorily take action or provide information or any such assistance as required to CERT-In. If the order/direction provide a format in which the information is required (up to and including near real-time), and a specified timeframe in which it is required, such directions must be complied with.

34 As per the CERT-In Rules, "Cyber security incident" means any real or suspected adverse event in relation to cyber security that violates an explicitly or implicitly applicable security policy resulting in unauthorized access, denial of service or disruption, unauthorised use of a computer resource for processing or storage of information or changes to data, information without authorization.

35 As per the CERT-In Rules, "Cyber incident" means any real or suspected adverse event that is likely to cause or causes an offence or contravention, harm to critical functions and services across the public and private sectors by impairing the confidentiality, integrity, or availability of electronic information, systems, services or networks resulting in unauthorised access, denial of service or disruption, unauthorised use of a computer resource, changes to data or information without authorisation; or threatens public safety, undermines public confidence, have a negative effect on the national economy, or diminishes the security posture of the nation.

36 See: https://www.cert-in.org.in/PDF/certinirform.pdf, last accessed on May 30, 2023.

C. KYC Requirements for Identified Service Providers

The Directions also contain certain 'know your customer' (KYC) requirements for specific entities such as data centres, cloud service providers,[37] virtual private network (VPN) service providers[38] and virtual private server (VPS) providers ("**Identified Service Providers**").[39] The terms "data centres", "cloud service providers", "VPN service providers" and "VPS providers" have not been defined under the Directions or CERT-In Rules.

If any Entity falls under the purview of Identified Service Providers, and provides services to customers in India, such entity must register the following accurate information which must be maintained by them for a period of 5 years or longer duration as mandated by the law after any cancellation or withdrawal of the registration as the case may be:

- Validated[40] names of subscribers/customers hiring the services
- Period of hire including dates
- IPs allotted to / being used by the members
- Email address and IP address and time stamp used at the time of registration / on-boarding
- Purpose for hiring services
- Validated address and contact numbers
- Ownership pattern of the subscribers / customers hiring services

The entity would be required to maintain, in a safe and secure manner, basic information about customers/ subscribers who use their services viz. individual, partnership, association, company etc. of whatsoever nature, with brief particulars of key management.

D. Additional Requirements

Additionally, certain KYC requirements are also applicable to virtual asset service providers, virtual asset exchange providers and custodian wallet providers ("**Virtual Asset Entities**").[41] However, there is no clarity under the Directions or FAQs on the definition or scope of such entities.

37 While there is no definition of "cloud service providers", based on oral clarifications from the Government, we understand that the scope of such entities will have to be determined on a case to case basis, inter alia depending on the nature of services provided by an entity, and arrangements of the entity with third party service providers.

38 For the purpose of the Directions, "VPN Service provider" refers to an entity that provides "Internet proxy like services" through the use of VPN technologies, standard or proprietary, to general Internet subscribers/users. This covers B2B and B2C VPN service providers. However, this does not include entities which provide VPN internally to its employees.

39 Paragraph (v) of the Directions.

40 The Government had indicated that additional clarity will be provided on the scope of the term "validated" as mentioned above, which may be specified to mean Aadhaar-based validation of customer names. However, this approach had not been finalized.

41 Paragraph (vi) of the Directions.

Applicability of CERT-In Rules and Directions to Indian and foreign Entities

The compliance requirements under the CERT-In Rules and Directions can be categorized into three broad categories (as detailed above):

I. Mandatory Ongoing Compliances

These are applicable to:

a. Entities having a computer,[42] computer system,[43] or computer network[44] (**"Computer Infrastructure"**) in India; and

b. Entities having Computer Infrastructure outside India, if there is a high probability that any incident which affects such Computer Infrastructure outside India also has an impact on any Computer Infrastructure in India (such as due to the nature of connectivity between these Computer Infrastructure).[45]

II. Conditional Compliances

These are applicable to:

a) All Entities having Computer Infrastructure in India; and

b) Entities which have Computer Infrastructure outside India, and such Computer Infrastructure is impacted by an incident which (I) in turn impacts the Entity's Computer Infrastructure located within the Indian territorial jurisdiction; or (II) originated in India.

III. KYC Requirements for Identified Service Providers

These are likely to be applicable to any Identified Service Provider which offers services to customers in India, irrespective of the location of the Computer Infrastructure, or the impact or origination of any incident which affects such Computer Infrastructure.

Penalty for Non-compliance

As compared to the CERT-In Rules, non-compliance with any provision under the Directions (including any other directions issued by CERT-In) entails a stricter punishment and may include imprisonment of up to one year and/or fine of up to INR 100,000 (approx. USD 1250).[46]

---

42 Defined under the IT Act as "*any electronic, magnetic, optical or other high-speed data processing device or system which performs logical, arithmetic and memory functions by manipulations of electronic, magnetic or optical impulses, and includes all input, output, processing, storage, computer software or communication facilities which are connected or related to the computer in a computer system or computer network*".

43 Defined under the IT Act as "*a device or collection of devices, including input and output support devices and excluding calculators which are not programmable and capable of being used in conjunction with external files which contain computer programmes, electronic instructions, input data and output data that performs logic, arithmetic, data storage and retrieval, communication control and other functions*".

44 Defined under the IT Act as "*the inter-connection of one or more computers or computer systems or communication device through-*

i) the use of satellite, microwave, terrestrial line, wire, wireless or other communication media; and

ii) terminals or a complex consisting of two or more inter-connected computers or communication device whether or not the inter-connection is continuously maintained."

45 There is no requirement for Entities outside India to comply with ongoing compliance requirements (such as appointment of a Point of Contact), unless such Entity owns any Computer Infrastructure in India. However, if there is a **high probability** that an incident which impacts any Entity's Computer Infrastructure outside India also impacts Computer Infrastructure within India (for e.g., due to the nature of connectivity) the Entity which owns such Infra should comply with the ongoing compliance requirements under the Directions and CERT-In Rules with respect to the relevant Computer Infrastructure outside India. This is because such Entity may generally be aware of the possibility of such an incident and its impact on Computer Infrastructure within India, irrespective of whether such an incident occurs or not.

46 Section 70B(7) of the IT Act.

D. CERT-In Advisories, Vulnerability Reports

CERT-In also collaborates with various researchers, cybersecurity organisations, academic institutions, vendors, etc. in addition to Computer Emergency Response Teams of other countries. To this end, CERT-In encourages reporting of vulnerabilities by various entities on a voluntary basis, as per the Responsible Vulnerability Disclosure and Coordination Policy.[47]

In vulnerability reports, CERT-In requires the following information to be provided:

i. The product(s) affected

ii. The exact software version or model affected;

iii. Vendor details

iv. Description of the vulnerability along with concise steps to reproduce the reported vulnerability along with supporting evidences such as:

- Proof of concept (PoC) and/or
- Code sample and/or
- Crash reports and/or
- Screenshots and Video recording etc.

v. The impact of exploiting the vulnerability.

Additional information may also be provided by the discloser on a voluntary basis.

Once the vulnerability report is provided, CERT-In examines and validates the vulnerability report and communicates to the discloser whether or not the report will be coordinated by CERT-In. Upon successful validation, CERT-In initiates coordination with the relevant product vendor(s), discloser and other stakeholders (if required) for the remediation and closure of the issue. Subsequently, CERT-In releases vulnerability notes/advisories on its website after the vulnerability is addressed. This is done in coordination with the relevant stakeholders. CERT-In is not permitted to disclose information which can identify individuals or organisations affected by cybersecurity incidents unless it has the express written consent of the relevant entity, or under orders of a competent Indian court.[48] This applies to both incident and vulnerability reports. However, CERT-In may disclose relevant information to any stakeholder, on the following grounds: (i) in the interest of sovereignty or integrity of India, (ii) defence of India, (iii) security of the State, (iv) friendly relations with foreign States; (v) public order. (vi) for preventing incitement to the commission of an offence relating to cognizable offences or (vii) enhancing cybersecurity in the country.[49]

CERT-In seeks to resolve issues brought to its notice within 120 days from contacting the relevant vendor, although these timelines may be affected due to various factors such as no response from vendor, the vulnerability being exploited actively, etc.

47 See: https://www.cert-in.org.in/RVDCP.jsp., last accessed on May 30, 2023.

48 Rule 13(1) of the CERT-In Rules.

49 Rule 13(4) of the CERT-In Rules.

CERT-In's support is prioritized based on the following factors (in a decreasing order):[50]

i) threats to the physical safety of human beings due to cybersecurity incidents;

ii) cyber incidents and cybersecurity incidents of severe nature (such as denial of service, distributed denial of service, intrusion, spread of computer contaminant,) on any part of the public information infrastructure including backbone network infrastructure;

iii) large-scale or most frequent incidents such as identity theft, intrusion into computer resource, defacement of websites etc.;

iv) compromise of individual user accounts on multi-user systems;

v) (v)types of incidents other than those mentioned above will be prioritised according to their apparent severity and extent.

Government's Powers to Intercept and Monitor Data

Section 69 of the IT Act provides for interception, monitoring and decryption powers of the Central Government if necessary in the interest of the sovereignty or integrity of India, defence of India, security of the State, friendly relations with foreign States or public order or for preventing incitement to the commission of any cognizable offence relating to the above or for investigation of any offence. Further, Section 69B authorizes an agency notified by the Central Government to monitor and collect traffic data or information through any computer resource for cybersecurity.

However, these powers are subject to safeguards which are prescribed under the Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009 ("**Interception Rules**") formulated under Section 87(2)(y) read with Section 69(2) of the IT Act.[51] The MeitY has authorized and designated the Director, NCCC as the 'Designated Officer' for issuing orders to carry out interception, monitoring or decryption of any information generated, stored, transmitted, etc. in any computer resource[52]

On December 30, 2018, the Ministry of Home Affairs ("**MHA**") issued a notification[53] under Section 69(1) of the IT Act read with Rule 4 of the Interception Rules authorizing 10 security and intelligence agencies[54] for the purposes of interception, monitoring, and decryption of any information generated, transmitted, stored, etc. in a computer resource. However, later a senior official of the MHA clarified that no "blanket powers" had been given to any new agencies. Instead, all agencies are still required to obtain prior approval from the Secretary of the MHA before intercepting any data stored on a computer.[55] The official also stated that the 10 agencies notified in the order were already empowered to intercept information since 2011. Therefore, the notification simply served to formally notify these agencies of their existing powers.[56]

50 Rule 11 of the CERT-In Rules.

51 See: https://www.meity.gov.in/writereaddata/files/Information%20Technology%20%28Procedure%20and%20Safeguards%20for%20Interception%2C%20Monitoring%20and%20Decryption%20of%20Information%29%20Rules%2C%202009.pdf, last accessed on May 05, 2023.

52 Rule 3, Interception Rules.

53 See: https://egazette.nic.in/WriteReadData/2018/194066.pdf, last accessed on April 18, 2023.

54 (i) Intelligence Bureau; (ii) Narcotics Control Bureau; (iii) Enforcement Directorate; (iv) Central Board of Direct Taxes; (v) Directorate of Revenue Intelligence; (vi) Central Bureau of Investigation; (vii) National Investigation Agency; (viii) Cabinet Secretariat (RAW); (ix) Directorate of Signal Intelligence (For service areas of Jammu & Kashmir, North-East and Assam only); (x) Commissioner of Police, Delhi.

55 Rule 4 of the Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009; See: https://www.indiatvnews.com/news/india-surveillance-order-centre-has-not-given-blanket-powers-to-agencies-every-action-requires-prior-approval-says-mha-496275, last accessed on April 18, 2023.

56 See: https://www.newindianexpress.com/nation/2018/dec/30/no-blanket-powers-to-10-agencies-to-intercept-every-action-requires-prior-approval-mha-1918405.html, last accessed on April 18, 2023.

E. Sectoral Regulations

Currently under Indian law, the financial and insurance sectors have separate cybersecurity guidelines, as discussed below.

I. RBI

The Reserve Bank of India ("**RBI**") has the power to issue directions and determine standards in relation to payment systems.[57] Below are the various types of entities that the RBI has power to govern or issue directions to, and the rules/frameworks that apply to each entity:

A. Banks

The RBI has prescribed cybersecurity guidelines under the various directions and standards issued by it. RBI has also notified a cybersecurity framework for banks ("**Bank Framework**")[58], including a separate framework for primary urban cooperative banks ("**UCB Framework**").[59]

The Bank Framework requires banks to:

- put in place a cyber-security policy providing an appropriate approach to combat cyber threats, basis the level of business complexity and risk, duly approved by the bank's Board.[60] This cybersecurity policy should be distinct and separate from the broader IT/security policy, to cover cyber threat risks and cover the measures to address/mitigate the risks.[61]
- a security operations centre should be set up, and this centre should undertake continuous surveillance and keep updated on the latest nature of emerging cyber threats.[62]
- a cyber crisis management plan should be a put in place and made part of the overall Board-approved strategy. This plan should cover detection, containment, response and recovery of cyber crises.[63]
- report all unusual cybersecurity incidents (whether successful or not) to the RBI.[64]
- The Bank Framework prescribes baseline cybersecurity and resilience requirements, which are indicative and is to be undertaken alongside the controls prescribed by CERT-IN.[65]

The requirement of approval of board of directors for certain policies indicates the importance of cyber-security measures. The director(s) of a company may be held liable for not acting in good faith while reviewing such policies, or not in the best interests of the company, under the Companies Act, 2013. The penalty is a fine of INR 100,000 – 500,000.[66]

57 Section 18 and 10(2) of the Payments and Settlement Systems Act, 2007, available at: https://rbidocs.rbi.org.in/rdocs/Publications/PDFs/86706.pdf, last accessed on May 30, 2023.

58 RBI Cyber Security Framework in Banks, 2016. See: https://www.rbi.org.in/Scripts/NotificationUser.aspx?Id=10435&Mode=0.

59 Comprehensive Cyber Security Framework for Primary (Urban) Cooperative Banks (UCBs) – A Graded Approach, available at: https://www.rbi.org.in/Scripts/NotificationUser.aspx?Id=11772&Mode=0, last accessed on May 30, 2023.

60 Clause 3, Bank Framework.

61 Clause 4, Bank Framework.

62 Clause 6, Bank Framework.

63 Clause 11 and 12, Bank Framework.

64 Clause 14, Bank Framework.

65 Annex 1, Bank Framework.

66 Section 166 of the Companies Act, 2013.

The UCB Framework prescribes various regulatory requirements. These requirements are applied in a varying manner to urban cooperative banks ("**UCB**"), with four levels of requirements prescribed based on the UCBs' functions.[67] Similar to the Bank Framework, baseline cybersecurity and resilience requirements, including additional requirements for each classification/level of UCBs, have been prescribed.[68]

Additionally, the RBI Master Direction on Digital Payment Security Controls, 2021[69] ("**MD-Digital Payment Security Controls**") requires all banks to implement multi-factor authentication for payments through electronic modes (except where the RBI has exempt such requirement, such as for recurring payments for up to INR 15,000), where at least one of the authentication methodologies should be dynamic e.g., use of OTPs. It is also recommended that banks adopt authentication based on the risk assessment of each type of payment method.

For prepaid payment instruments ("**PPI**")[70], the security and risk management framework require the PPI issuer to establish a mechanism for monitoring, handling and follow-up of cybersecurity incidents and cybersecurity breaches. The same should be reported immediately to the Department of Payments and Settlement Systems ("**DPSS**"), RBI. It is also required to be reported to CERT-In[71] Additionally, non-bank PPI issuers should submit a system audit report including a cybersecurity audit conducted by a CERT-IN empaneled auditor, within two months of the close of its financial year to the respective regional office of the DPSS, RBI.[72]

For Banks engaging with lending service providers and offering digital lending apps, the RBI Digital Lending Guidelines, 2022 ("**Digital Lending Guidelines**")[73] has prescribed technology standards that require regulated entities that undertake digital lending (i.e. banks, "RE") to ensure that REs and the lending service providers engaged by them (i.e. an agent of a RE that aids with some lending functions) comply with various technology standards/ requirements on cybersecurity stipulated by the RBI and other agencies.[74]

The RBI Master Direction on Credit Card and Debit Card Issuance and Conduct, 2022[75] ("**Debit and Credit Card MD**") applies to banks issuing credit cards and debit cards, and provides compliances to be undertaken by the card issuer for online safety. The issue of cards as a payment mechanism is also subject to relevant instructions on security issues and risk mitigation measures issued by the DPSS, RBI, and the Foreign Exchange Department, RBI under Foreign Exchange Management Act, 1999, as amended from time to time.[76] Card-issuers are not permitted to reveal any information relating to customers to any other person/organization without obtaining their explicit consent, for the purposes for which the information will be used and the organizations with whom the information will be shared. In cases where the customers give explicit consent for sharing the information, card-issuers are to explicitly provide the customer with the full meaning/implications of the disclosure clause.

---

67 Clause 2, Comprehensive Cyber Security Framework for Primary (Urban) Cooperative Banks (UCBs) – A Graded Approach.

68 Annex I and II, Comprehensive Cyber Security Framework for Primary (Urban) Cooperative Banks (UCBs) – A Graded Approach.

69 RBI Master Direction on Digital Payment Security Controls, 2021, available at: https://rbi.org.in/scripts/NotificationUser.aspx?Mode=0&Id=12032, last accessed on April 7, 2023.

70 RBI Master Directions on Prepaid Payment Instruments ("**PPI-MD**"), available at: https://www.rbi.org.in/Scripts/BS_ViewMasDirections.aspx?id=12156, last accessed on May 30, 2023.

71 Clause 15.7, PPI-MD.

72 Clause 18, PPI-MD.

73 RBI Digital Lending Guidelines, 2022, available at: https://rbidocs.rbi.org.in/rdocs/notification/PDFs/GUIDELINESDIGITALLENDINGD5C35A71D8124A0E92AEB940A7D25BB3.PDF, last accessed on May 30, 2023.

74 Clause 13 of the Digital Lending Guidelines.

75 RBI Master Direction – Credit Card and Debit Card – Issuance and Conduct Directions, 2022. See: https://rbi.org.in/Scripts/BS_ViewMasDirections.aspx?id=12300, last accessed on May 30, 2023.

76 Clause 25, Debit and Credit Card MD.

The information sought from customers should not violate the provisions of law relating to maintenance of secrecy in the transactions. Similarly, under a co-branding arrangement, the co-branding entity is not be permitted to access any details of the customer's accounts that may violate the card-issuer's secrecy obligations.[77]

The RBI Master Direction on KYC, 2016[78] ("**KYC MD**") lays down the manner in which KYC can be conducted by REs. In 2021, the KYC MD was updated to include Video based Customer Identification Process ("**V-CIP**") as a method for completing KYC.

The following compliances are required under the KYC MD:

- In undertaking V-CIP, the RE should comply with the RBI Bank Framework and other general guidelines on IT risks.
- The V-CIP connection and interaction needs to originate from the RE's own secured network domain and ensure end-to-end encryption of data between the customer device and the hosting point of the V-CIP application.
- Customer consent should be recorded in an auditable and alteration-proof manner.
- In case of any detected case of forged identity through V-CIP, the same should be reported as a cyber event under extant regulatory guidelines.
- The V-CIP infrastructure needs to undergo necessary tests such as vulnerability assessment and penetration tests ("**VAPT**") and a security audit to ensure its robustness and end-to-end encryption capabilities.
- REs are required to ensure Aadhaar numbers are redacted or blacked out.
- The entire data and recordings of V-CIP has to be stored by REs in a system located in India.[79]

B. Prepaid Payment Instrument Issuers

For payment system operators that are not banks, compliances detailed on page 23 of this Paper under the Bank Framework and the UCB Framework would apply. Further, the KYC MD would also be applicable.

C. Payment Aggregators

The RBI Guidelines on Regulation of Payment Aggregators and Payment Gateways, 2020[80], provide baseline technology-related recommendations ("**Technology Recommendations**"). These Technology Recommendations are mandatory for payment aggregators and not mandatory, although prescribed as a good practice, for payment gateways. Payment Aggregators are entities that facilitate acceptance by e-commerce sites and merchants, of various payment instruments from the customers for completion of their payment obligations without the need for merchants to create a separate payment integration system of their own. Payment gateways are entities that provide technology infrastructure to route and facilitate processing of an online payment transaction without any involvement in handling of funds.

77 Clause 27 Debit and Credit Card MD.

78 Master Direction - Know Your Customer (KYC) Direction, 2016. See: https://www.rbi.org.in/Scripts/BS_ViewMasDirections.aspx?id=11566, last accessed on May 30, 2023.

79 Clause 18, KYC MD.

80 RBI Guidelines on Regulation of Payment Aggregators and Payment Gateways, available at: https://www.rbi.org.in/Scripts/NotificationUser.aspx?Id=11822, last accessed on May 30, 2023.

The Technology Recommendations require that entities carry out a comprehensive security risk assessment of their people, IT, business process environment, etc., These can be an internal annual security audit by an independent security auditor or by a CERT-In empanelled auditor.[81] Entities must report security incidents/ card holder data breaches to the RBI within the stipulated timeframe, and a monthly cybersecurity incident report with root cause analysis and preventive actions undertaken is to be submitted to RBI.[82] Further, the KYC MD would also be applicable.

The entity's board approved information security policy has to be reviewed at least annually, considering alignment with business objectives; the objectives, scope, ownership and responsibility for the policy; information security organisational structure; information security roles and responsibilities, etc.[83] The entities must prepare a comprehensive cyber crisis management plan approved by the entity's IT Committee and has to include components such as detection, containment, response and recovery of cyber crises.[84]

II. SEBI

The Securities and Exchange Board of India ("**SEBI**") has released circulars on Cyber Security and Cyber Resilience Frameworks, with the frameworks laid down separately for mutual fund asset management companies, stock brokers, derivative exchanges, stock exchanges, clearing corporations, depositories, and share transfer agents.[85]

The circulars require the following:

- A cybersecurity and cyber resilience policy document for each entity, approved by the relevant officials of an organization that should cover assets and risks, detection and responses to anomalies, and a recovery mechanism for incidents.[86]
- The relevant officials should constitute an internal technology committee comprising of experts who are to review the policy on a half-yearly basis.
- A designated officer ("**DO**") should be appointed to identify risks according to the cybersecurity and cyber resilience policy of the entity, and periodically review any instances of cyber-attacks.[87]
- The entity must have a reporting procedure to facilitate communication of unusual activities to the DO.[88]
- There must be a response plan to define these roles, and periodic drills must be performed to test the effectiveness of the recovery plan.

---

81 Clause 1.1, RBI Guidelines on Regulation of Payment Aggregators and Payment Gateways.

82 Clause 1.3, RBI Guidelines on Regulation of Payment Aggregators and Payment Gateways.

83 Clause 1.6, RBI Guidelines on Regulation of Payment Aggregators and Payment Gateways.

84 Clause 1.7.4, RBI Guidelines on Regulation of Payment Aggregators and Payment Gateways.

85 The SEBI Cyber Security and Cyber Resilience framework of National Commodity Derivatives Exchanges, Mutual Fund Asset Management Companies, Stock Brokers, Stock Exchanges, Clearing Corporations, Depositories, and Share Transfer Agents, available at: https://www.sebi.gov.in/legal/circulars/jan-2019/cyber-security-and-cyber-resilience-framework-for-mutual-funds-asset-management-companies-amcs-_41589.html; https://www.sebi.gov.in/legal/circulars/oct-2019/cyber-security-and-cyber-resilience-framework-for-qualified-registrars-to-an-issue-share-transfer-agents_44660.html; https://www.sebi.gov.in/legal/circulars/jul-2015/cyber-security-and-cyber-resilience-framework-of-stock-exchanges-clearing-corporation-and-depositories_30221.html; https://www.sebi.gov.in/legal/circulars/mar-2016/cyber-security-and-cyber-resilience-framework-of-national-commodity-derivatives-exchanges_32150.html; https://www.sebi.gov.in/legal/circulars/sep-2017/cyber-security-and-cyber-resilience-framework-for-registrars-to-an-issue-share-transfer-agents_35890.html; https://www.sebi.gov.in/legal/circulars/dec-2018/cyber-security-and-cyber-resilience-framework-for-stock-brokers-depository-participants_41215.html; and https://www.sebi.gov.in/legal/circulars/dec-2018/cyber-security-and-cyber-resilience-framework-of-stock-exchanges-clearing-corporations-and-depositories_41244.html, last accessed on May 30, 2023.

86 Clause 2, SEBI Cyber Security and Cyber Resilience framework of Stock Brokers.

87 Clause 7, SEBI Cyber Security and Cyber Resilience framework of Stock Brokers.

88 Clause 8, SEBI Cyber Security and Cyber Resilience framework of Stock Brokers.

- Physical access to critical systems must be restricted and revoked if not required.
- There must be baseline standards to facilitate the consistent application of security configurations to operating systems and databases which must be secured in the entity's facilities with proper access controls.[89]
- There must be mechanisms to monitor the capacity utilization of critical systems and networks being exposed to the internet. Any alerts that come from the monitoring mechanisms must be properly investigated to know what measures are to be taken to prevent future attacks.[90]

Qualified registrars and transfer agents and market infrastructure institutions are mandated to conduct comprehensive cyber audits at least twice in a financial year.[91] All cyber-attacks, threats, cyber-incidents and breaches experienced by stock brokers, registrars and transfer agents and market infrastructure institutions must be reported to SEBI within 6 hours of detecting such incidents or being brought to notice about such incidents, and to CERT-In in accordance with the relevant guidelines detailed above in Section 3.[92] Quarterly reports containing information on threats and cyber-incidents that may be useful to other stock brokers, registrars and transfer agents and market infrastructure institutions must be submitted to SEBI within 15 days from the quarters ending June, September, December and March of every year. [93]

For algorithmic trading facilities, proper measures must be undertaken to isolate and secure the perimeter and server connectivity. [94] Application security for customer facing applications offered over the internet containing sensitive information must also be secured, and the responsibility of ensuring cyber resilience on those applications resides with the market infrastructure institutions and not with the stock-broker/depository participant.[95]

In case of any technical glitches faced by a stock broker (a technical glitch is any malfunction in the systems of a stock broker including malfunction in its hardware, software, networks, processes or any products or services provided by the stock broker online)[96], stock brokers have to report these to stock exchanges immediately but not later than 1 hour from the time of occurrence. Stock-brokers must also submit a report of the technical glitch to the stock exchange within 14 days from the date of the incident, and appropriate action must be taken by the stock exchanges.[97]

89 Clauses 22-24, SEBI Cyber Security and Cyber Resilience framework of Stock Brokers.

90 Clause 46, SEBI Cyber Security and Cyber Resilience framework of Stock Brokers.

91 Paragraph 2, SEBI Circular to All Qualified Registrars/Share Transfer dated July 6, 2022.

92 Clause 2, SEBI Circular on Cyber Security and Cyber Resilience framework of for Stock Brokers/Depository Participants.

93 Clause 2, SEBI Circular to All Qualified Registrars/Share Transfer Agents.

94 Clause 26, SEBI circular on Cyber Security & Cyber Resilience framework for Stock Brokers / Depository Participants.

95 Clause 57, SEBI circular on Cyber Security & Cyber Resilience framework for Stock Brokers / Depository Participants.

96 Clause 2.1, SEBI circular on Framework to address the 'technical glitches' in Stock Brokers' Electronic Trading Systems, available at: https://www.sebi.gov.in/legal/circulars/nov-2022/framework-to-address-the-technical-glitches-in-stock-brokers-electronic-trading-systems_65466.html, last accessed on May 30, 2023.

97 Clause 3.2 and 3.3, SEBI circular on Framework to address the 'technical glitches' in Stock Brokers' Electronic Trading Systems.

III. IRDAI

The Insurance Regulatory and Development Authority ("**IRDAI**") issued the Guidelines on Information and Cyber Security ("**IRDAI Guidelines**").[98] This applies to all insurers regulated by the IRDAI as of 2017,[99] and has been extended to all insurance intermediaries (including brokers, corporate agents, web aggregators, corporate surveyors, insurance self-networking platforms and insurance repositories) as of 2022.[100]

Insurance intermediaries are required to implement the IRDAI Guidelines in a phased manner as stated below:

- the appointment of a Chief Information Security Officer ("**CISO**") and preparing a gap analysis report has to be completed by December 31, 2022, and
- the cybersecurity assurance program to close gaps as per the annual assurance audit has to be completed by March 31, 2023.
- Moreover, the insurers are required to:
- Set out a cyber-security management program ("**Cyber Security Policy**") covering ongoing processes, control improvements, and state-of-the-art network policies and procedures. The risks to the insurers' information and related processes from involving external parties must be identified and appropriate controls are to be put in place;[101]
- Appoint an Information Security Committee to review and approve exceptions to the Cyber Security Policy, and any significant risk is to be reported to the Board of the insurer;[102]
- Appoint a CISO, who will be responsible for providing advice and support to the management and informing users of the implementation of the Cyber Security Policy;[103]
- Carry out an independent assurance audit annually by a qualified external systems auditor holding relevant certifications, or by a CERT-IN empaneled auditor;[104]
- Submit a closure report to the IRDAI within two months of the completion of the assurance audit;[105]
- Define security perimeters which would be used to protect areas that contain sensitive or critical information, both online and offline;
- Regularly review, update and revoke, when necessary, the access rights to secure areas;
- Protect IT equipment from power failures and other disruptions caused by failures in supporting utilities.[106]

98 See: https://www.aicofindia.com/AICEng/General_Documents/Notices%20And%20Tenders/IRDAI-GUIDELINES.pdf, last accessed on May 30, 2023.

99 Clause 3, IRDAI Guidelines.

100 IRDAI circular on 'Implementation of Information and Cyber Security Guidelines' dated October 11, 2022, available at: https://irdai.gov.in/documents/37343/365525/Implementation+of+Information+and+Cyber+Security+Guidelines.pdf/cde08dbd-5337-f322-e541-143f9d96ace0?version=1.0&t=1666363225650&download=true, last accessed on May 30, 2023.

101 Clause 13.2, IRDAI Guidelines.

102 Clause 5.5, IRDAI Guidelines.

103 Clause 5.3 & 5.4, IRDAI Guidelines.

104 Clause 23.1, IRDAI Guidelines.

105 Clause 23.5(f), IRDAI Guidelines.

106 Clause 7, IRDAI Guidelines.

Additionally, an amendment to the IRDAI Guidelines in 2017 prescribes that vulnerability assessment and penetration tests ("**VAPT**") should be conducted by insurers on a periodic basis:[107]

- VAPT of ICT infrastructure should be conducted annually, and of all internet-facing applications should be conducted once in six months.
- Identified gaps in internet-facing applications must be resolved within one month of identification, and within two months for other applications.
- If a high-risk issue is not resolved within the timeline, it must be reported to the insurer's Board's Risk Management Committee.[108]

On April 24, 2023, the IRDAI issued the revised Information and Cyber Security Guidelines, 2023[109] in light of the growing use of digital technologies and the subsequent rise in cybersecurity breaches. The revised guidelines aim to assist the insurance industry in enhancing their protective measures and governance protocols for addressing the emerging cyber risks. The updated guidelines are applicable to all insurers, including insurance intermediaries such as brokers, corporate agents, web aggregators, insurance repositories, Insurance Information Bureau of India (IIB), etc. Entities that have undergone a security audit for FY 2022-23 are required to comply with the Guidelines starting from the next fiscal year.

F. The Digital Personal Data Protection Bill 2022

MeitY published the Digital Personal Data Protection Bill, 2022 ("**DPDPB**") for public consultation on November 18, 2022. The DPDPB is a proposed piece of legislation in India that aims to regulate the collection, use, and processing of personal data by organizations in the country. Marking a significant change from its predecessor drafts, the DPDPB is more open ended, leaving much to be prescribed by the Central Government.

With respect to cybersecurity, the DPDPB, *inter alia*, seeks to establish a framework for the protection of personal data, including provisions for data privacy, data security, and data breaches. It obligates[110] the Data Fiduciary[111] or the Data Processor[112] to notify the Data Protection Board[113] (i.e. the proposed adjudicatory body for the enforcement of the DPDPB) and the affected Data Principals[114] in the event of a personal data breach.[115] The Board may then direct the Data Fiduciary to adopt any urgent measures to remedy such personal data breach or mitigate any harm caused to Data Principals.[116]

107 Clause 14.1, IRDAI Guidelines.

108 Clause 5.5(h), IRDAI Guidelines.

109 See: https://irdai.gov.in/document-detail?documentId=3314780, last accessed on May 04. 2023.

110 Section 9(5) of the DPDPB.

111 As per Section 2(5) of the DPDPB, Data Fiduciary means "any person who alone or in conjunction with other persons determines the purpose and means of processing of personal data."

112 As per Section 2(7) of the DPDPB, Data Processor means "any person who processes personal data on behalf of a Data Fiduciary."

113 As per Section 2(2) of the DPDPB, Board means "the Data Protection Board of India established by the Central Government for the purposes of the Act."

114 As per Section 2(6) of the DPDPB, Data Principal means "the individual to whom the personal data relates and where such individual is a child includes the parents or lawful guardian of such a child."

115 As per Section 2(14) of the DPDPB, Personal Data Breach means "any unauthorised processing of personal data or accidental disclosure, acquisition, sharing, use, alteration, destruction of or loss of access to personal data, that compromises the confidentiality, integrity or availability of personal data."

116 Section 20(3) of the DPDPB.

Apart from the above, Data Fiduciaries and Data Processors are required to protect the personal data in its possession by taking reasonable security safeguards to protect against any personal data breaches.[117] Similarly, a Significant Data Fiduciary[118] must undertake additional measures including a 'Data Protection Impact Assessment'[119] to assess the potential risks and harms involved before undertaking any high-risk processing of personal data.

Hence, the DPDPB does not prescribe specific standards to be adopted for the purpose of maintaining security. Instead, it is left to the concerned entity to determine the appropriate technology and measures necessary to ensure compliance with the requirement to maintain reasonable security standards.

The DPDPB also prescribes a penalty of up to INR 250 crore in case of any failure of Data Processor or Data Fiduciary to take reasonable security safeguards to prevent personal data breach, and a penalty of up to INR 200 crore in case of a failure to notify the Board and affected Data Principals in the event of a personal data breach.[120]

The industry has pushed back on this requirement since the CERT-In Directions from 2022 already require mandatory reporting of cybersecurity incidents, which would include personal data breaches. Failure to report incidents under the CERT-In Directions are punishable with imprisonment and/or fine and the penal provisions under the DPDPB would lead to duplicity of punishments for the same breach.

G. Other Government Efforts

Apart from the above, the Government has undertaken numerous measures towards improving cyber-security of India. The prevention of cybercrimes is being handled through seven departments under the Indian Cyber Crime Coordination Centre ("**I4C**") and Cyber and Information Security division of Ministry of Home Affairs.[121] Further, efforts have been made to create awareness amongst the people through various steps like measures for prevention of cybercrimes, popularization of crime reporting portal, development of Cybersafe which is an application developed jointly by Fake Indian Currency Coordination Group ("**FCORD**") and the private sector with the objective of making the digital payment eco-system safe and secure, enhancing the faith of the common man in the platform, and assisting law enforcement agencies in resolving and preventing all such crimes.[122] and the financial cybercrime reporting helpline number.

The Government has also trained more than 16,000 police officers across the country through the CyTrain portal for responding to cybercrime.[123]

117 Section 9(4) of the DPDPB.

118 The Central Government may classify a Data Fiduciary or a class of Data Fiduciary as a Significant Data Fiduciary based on the volume and sensitivity of the data processed by them, the risk of harm to the data principal, potential impact on the sovereignty and integrity of India and other such factors; Refer to Section 11(1) of the DPDPB.

119 As per Section 11(2)(c), Data Protection Impact Assessment means "a process comprising description, purpose, assessment of harm, measures for managing risk of harm and such other matters with respect to processing of personal data, as may be prescribed."

120 Schedule 1 of the DPDPB.

121 These are namely, National Cyber Crime Threat Analytics Unit, National Cyber Crime Reporting Portal, National Cyber Crime Training Centre, National Cyber Crime Research and Innovation Center, Joint Cyber Crime Coordination, National Cyber Crime Ecosystem Management Unit and National Cyber Crime Forensic Laboratory.

122 See: https://cybersafe.gov.in/Cybersafe/index.html, last accessed on May 30, 2023.

123 See: https://www.pib.gov.in/PressReleasePage.aspx?PRID=1835559, last accessed on May 30, 2023.

Treaties for Cybersecurity Co-operation

India has entered into several bilateral treaties with other countries for cybersecurity co-operation and capacity building in the cyberspace, some of which are discussed below.

I. UK

In May 2021, the Indian and UK governments had agreed to an "Enhanced Cyber Security Partnership" which was further emphasized in 2022 and would be focused on cyber governance, deterrence, resilience and capacity building.[1] As a part of this partnership, both countries agreed to "deepen co-ordination on mitigation strategies against Advanced Persistent Threats as well as cooperation on tackling cybercrime".

II. US

In 2011, a memorandum of understanding[2] was signed between MeitY and the Department of Homeland Security, Government of the United States of America ("**DHS**"), for promotion of closer cooperation and timely exchange of information between the organizations. In 2017, a new memorandum of understanding was signed between MeitY and the DHS on cooperation in the field of cybersecurity, which was further renewed in 2018. It is reported that CERT-In and the US CERT share information and discuss cybersecurity related issues as and when required.[3]

III. Japan

In 2020, India and Japan signed a memorandum of cooperation in the field of cybersecurity, to enhance cooperation in areas such capacity building in the cyberspace, protection of critical infrastructure, cooperation in emerging technologies, sharing information on cybersecurity threats, and malicious cyber activities, as well as best practices to counter them. The agreement is aimed to promote cooperation in key areas such as 5G networks, artificial intelligence, internet of things, etc. The aim is for an open, interoperable, free, secure and reliable cyberspace environment and to promote the internet as an engine of innovation, economic growth, and trade and commerce, in accordance with respective domestic laws.[4]

1 See: https://www.gov.uk/government/publications/prime-minister-boris-johnsons-visit-to-india-april-2022-uk-india-joint-statements/india-uk-cyber-statement-april-2022, last accessed on May 30, 2023.

2 See: https://www.dqindia.com/india-cert-signs-an-mou-with-us-cert/, last accessed on May 30, 2023.

3 See: https://economictimes.indiatimes.com/news/defence/india-us-renew-agreement-for-cyber-security-coordination/articleshow/56484102.cms?from=mdr, last accessed on May 30, 2023.

4 See: https://indbiz.gov.in/india-japan-sign-memorandum-of-cooperation-in-the-field-of-cybersecurity/, last accessed on May 30, 2023.

IV. China

The Government of India has, in the past, committed to cooperation and information sharing with respect to cybercrime with China. In 2005, the MHA and the Ministry of Public Security of China ("**MPS**") had signed a memorandum of understanding which *inter alia included commitments on exchanging information with respect to cybercrime.*[5] In 2015, MHA and MPS had issued a joint statement committing to strengthen cooperation in combating terrorism and cybercrimes and other fields, and also encourage the long-term, healthy and stable development of law enforcement cooperation between the two countries.[6] In 2018, India and China signed a first-ever agreement on security cooperation to strengthen and consolidate assistance in counter-terrorism, organised crimes, etc. and exchange of information.[7]

V. Russia

In 2015, India had issued a joint declaration with Russia which included within its scope bilateral cooperation in the field of ICT.[8] This was followed by an agreement signed between Russia and India in 2016 on cooperation in tackling cybercrime, and a further reiteration by the two countries in 2018 with respect to the need for more practical cooperation *inter alia on issues relating to ensuring security in the use of ICTs, including information sharing on emerging threats in this field.*

5 See: http://www.mea.gov.in/Portal/LegalTreatiesDoc/CH05B0622.pdf, last accessed on May 30, 2023.

6 See: https://pib.gov.in/newsite/PrintRelease.aspx?relid=131765, last accessed on May 30, 2023.

7 See: https://www.hindustantimes.com/india-news/india-china-sign-first-security-cooperation-agreement/story-TvHK1dqJGi4Kz2JS8CdScJ.html, last accessed on May 30, 2023.

8 See: https://mea.gov.in/outoging-visit-detail.htm?26243/Joint+Statement+between+the+Russian+Federation+and+the+Republic+of+India+Shared+Trust+New+Horizons+December+24+2015, last accessed on May 30, 2023.

Guidance for Decisions and Actions

Cybersecurity risks are real risks with significant operational, strategic, financial, reputational, and legal implications. Organizations need to create awareness about and undertake adequate measures at every level, starting from the Board of Directors to Chief Information Security Officer (CISO) to functional and business unit managers. While these measures may not eliminate the risks of cyberattacks, they can help significantly reduce them as well as provide immediate and effective response to a cyberattack. Here, we provide guidance for the Board of Directors and C-Suite/CISO Executives.

A. For the Board of Directors

It is not expected for the Board of Directors to be familiar with technical aspects of cybersecurity. However, the Board is expected to recognize the importance of cybersecurity and the impact of various types of cyber-attacks having material effects on the operations of the company. The Board must know whether the company is prepared to detect and stop a cyberattack and, when one does happen, how fast it can mitigate the effects and return to normal operations. Due diligence and an active role from the Board are a necessity now.

Corporate Cybersecurity Policy

The Board should require the management to establish and enforce strict policies to identify and protect against various sources and types of cyberattacks. Cybersecurity policies and procedures must be clearly documented and disseminated across the company ensuring that every employee knows his or her role in ensuring cybersecurity.

These policies should include procedures for action when there is a cyberattack and personnel responsible for coordination within various units of the company as well as with relevant external stakeholders, suppliers, customers, enforcement agencies and regulators. Such policy should also be extended for handling sensitive data, including guidelines for accessing, storing, and transmitting data.

The Board also needs to prescribe situations when the entity needs to retain outside counsel, who specializes in cybersecurity and is able to provide responses to regulatory requirements and reduce reputational damages. In addition, the Board should undertake the requirement for the management to work with a trusted managed security service provider (“**MSSP**”) who can provide expert guidance and support to help organizations improve their cybersecurity posture.

Create a Subcommittee of the Board

In many businesses, for example, banking, insurance, logistics, payment services, transportation, etc., cyberattacks can significantly hamper the operations and may even bring the entire business to a halt. With digital transformation of traditional industries such risks have increased exponentially.

The Board must seriously assess the risk of cyberattacks on the company. When they find that the cyber-attacks can have mission-critical impacts, a Board-level subcommittee for cybersecurity must be appointed to prepare for and get activated in a crisis. The subcommittee should work with the management to establish and operationalize a cybersecurity group in the company.

The CISO should provide periodic reports on the readiness of the company as well as immediately inform the subcommittee when a certain level of cyberattack has occurred. A survey by the Ponemon Institute states 47% of the organizations have not assessed the readiness of their incident response teams.[1]

Another important role for the sub-committee is to monitor and regularly review the stress levels of the key personnel responsible for cybersecurity within the company. Multiple studies have found the extremely high level of stress and burnout among the experienced, high-level cybersecurity personnels, including CISOs.[2] Any change of personnel, excessive unavailability due to mental health situations, or staffing constraints in the cybersecurity group can have organization-wide implications and unduly expose the organization to cyberattacks. Often stress arises not from technological issues but from regulatory pressures. CISOs may be well-versed in technological shortcomings but they need to be supported and protected by the Board on the regulatory implications and requirements.

Cyber Insurance

For some companies, cyberattacks can lead to significant business disruption, financial losses, reputation damage, loss of future business, and other damages. The board needs consider cyber insurance, a type of insurance that provides coverage for various damages resulting from cyberattacks and other digital threats.

Cyber insurance provides coverage for businesses against a wide range of cyber-related risks, including data breaches, cyberattacks, business interruption, and damage to reputation. In addition, some cyber insurances also protect corporate officers from personal liability. There are several factors to be considered while purchasing cyber insurance, including the range of activities and liabilities covered, the level of coverage provided, the exclusions and limitations, and the cost of the policy. The cost of such policies varies basis the size and nature of the business, as well as the level of coverage being purchased.

While evaluating the insurance cover, the entities should also examine the obligations undertaken by it under various third-party contracts. In addition, a measure of risk, the board should require to the company to identify key supply-chain entities both upstream and downstream of the company's business and require those entities to subscribe to cyber insurance to minimize impact on cyberattacks in other parts of the company's supply chain.

1 Dr. Keri Pearlson et al, Cyberattacks Are Inevitable. Is Your Company Prepared?, Harvard Business Review (March 2021), Available at: https://hbr.org/2021/03/cyberattacks-are-inevitable-is-your-company-prepared, last accessed on May 30, 2023.

2 See: Strupp, Catherine (2023, May 17) "Cybersecurity Leaders Suffer Burnout as Pressures of the Job Intensify" *The Wall Street Journal,* https://www.wsj.com/articles/cybersecurity-leaders-suffer-burnout-as-pressures-of-the-job-intensify-b0609ef1, last accessed on May 21, 2023; Proofpoint (2023) "White Paper: 2023 Voice of the CISO", https://www.proofpoint.com/us/resources/white-papers/voice-of-the-ciso-report, last accessed on May 21, 2023; Caminity, Susan (2022, Sept 9) "Chief information security officers say stress and burnout, not job loss as a result of a breach, are their top personal risks" CNBC, last accessed on May 21, 2023.

B. For C-Suite/CISO Executives

C-Suite executives, in particular CISO, play the most important role in preparing the company for cybersecurity. While they need to be conversant with the technological shortcomings and potential weaknesses in their digital infrastructure, they also need to be familiar with legal and regulatory requirements related to cybersecurity.

Implementing Security Standards

The first step is to establish and undertake the due care to protect the company, including its employees, customers, suppliers and other stakeholders from potential cyberattacks. Depending upon the type of entity in question, there are various security standards that organizations can implement to improve their cybersecurity posture. Some common ones include:

i. **IS/ISO/IEC 27001**[3]: This is the Indian version of the ISO 27001 standard, which is an international standard for information security management systems ("**ISMS**"). It outlines a set of best practices and guidelines for implementing and maintaining a secure ISMS. This can help organizations understand the risks and vulnerabilities associated with their information assets and take appropriate measures to address the same.

ii. **PCI DSS**: The Payment Card Industry Data Security Standard[4] ("**PCI DSS**") is a set of security standards designed to ensure the secure handling of credit card information by merchants and service providers. In India, PCI DSS is applicable to all merchants and service providers that accept, process, transmit, or store cardholder data. It aims to ensure that these organizations implement certain technical and operational controls in order to protect the cardholders' data.

iii. **NIST Cybersecurity Framework**[5]: The National Institute of Standards and Technology ("**NIST**") Cybersecurity Framework ("**CSF**") is a voluntary framework that that provides guidance for managing cybersecurity risks. It is designed to be flexible and scalable, so it can be customized to meet the specific needs of an organization. The NIST CSF consists of five core functions: identify, protect, detect, respond, and recover. These functions represent the key activities that organizations should consider when developing and implementing a cybersecurity program.

Educating Employees and Creating Readiness

Having standardized policies by themselves is not sufficient, the executives must educate employees to create awareness about the importance of cybersecurity. Employee readiness is an important aspect of maintaining cybersecurity in an organization.

Employees are often the first line of defense against cyber threats, and if they are not aware of the risks and how to protect against them, it can significantly increase the risk of a cyberattack.

3 See: https://www.iso.org/isoiec-27001-information-security.html#:~:text=ISO%2FIEC%2027001%20is%20the,the%20ISO%2FIEC%2027000%20family, last accessed on May 30, 2023.

4 See: https://www.pcisecuritystandards.org/standards/, last accessed on May 30, 2023.

5 See: https://www.nist.gov/cyberframework/frequently-asked-questions/framework-basics#framework, last accessed on May 30, 2023.

When a cyberattack happens the fallout is usually very fast, preparing employees to immediately take the prescribed actions can help the company react quickly and mitigate the threat.

i. **Conduct regular training**: Provide employees with regular training on cybersecurity best practices. It is important to encourage a culture of security by raising awareness of the following:

   - Identification and prevention of phishing attacks and malware;
   - Creation and usage of strong passwords;
   - Potential consequences of a cyberattack, such as financial losses, reputational damage, and legal liabilities, to motivate them to take cybersecurity seriously;
   - Safe browsing practices, such as avoiding unknown or suspicious websites and links;
   - Reporting of suspicious activity or potential threats, and reward those who demonstrate good cyber-security practices.[6]

   It may be beneficial to use interactive training methods, such as role-playing, simulations and using real-life examples, to make the training more engaging and effective.[7]

ii. **Communicate policies and procedures**: Clearly communicate the organization's cybersecurity policies and procedures to employees, including what is expected of them in terms of protecting sensitive data and responding to threats.

iii. **Test employee knowledge**: Use quizzes, tests, and other assessment tools to test employee knowledge and identify areas where additional training is needed.

Technical Measures to Minimize Cybersecurity Risk

By undertaking adequate technical measures for maintaining cybersecurity, organizations can significantly reduce their risk of cyber-attacks. The implementation of these practices is an ongoing process and they can range from having policies, procedures and technical tools to authenticate access, protect data, protect network, protect digital assets and regularly conduct cybersecurity audit.

Access Authentication

i. Use strong, unique passwords for all accounts and regularly update them;

ii. Enable two factor authentications on all accounts to add an extra layer of security;

iii. protect their sensitive data from being compromised or stolen by unauthorized individuals.

6 Raza, M., How companies can train employees for a cyberattack, Forbes Magazine (October 2021), Available at: https://www.forbes.com/sites/forbesbusinesscouncil/2021/10/07/how-companies-can-train-employees-for-a-cyberattack/?sh=2bcce7251377, last accessed on May 30, 2023.

7 Panel, E., "Eight ways to train staff about Workplace Cyber Threats", Forbes Magazine (April 2022), Available at: https://www.forbes.com/sites/forbeshumanresourcescouncil/2022/04/14/eight-ways-to-train-staff-about-workplace-cyber-threats/?sh=7dc52e052d7a, last accessed on May 30, 2023.

Data Protection

i. Encrypt all sensitive data to prevent the same from unauthorized access, theft, and tampering;

ii. Back up important data regularly to a secure location to prevent data loss in the event of a data breach or ransomware attack;

Network Protection

i. Use content filtering solutions to block access to potentially malicious websites and protect against phishing attacks;

ii. Most companies allow BYOD (Bring Your Own Device). External devices may introduce certain device-level cybersecurity issues as the organization do not have full control over the employees' personal devices. Such devices may not have the same level of security measures as company-provided devices which can also make personal devices an entry point for illegal access to company network and make them more prone to data leakage.[8]

Digital Asset Protection

i. Install all security software (such as firewalls, antivirus, etc.) for protection against malware and other cyber threats. It is also important to ensure that these programs are regularly updated to protect against latest threats;

ii. Use cold wallets to hold cryptocurrency and virtual digital assets (i.e. on any platform or device not connected to the internet); and

Cybersecurity Audit

i. Conduct routinely security assessments to identify and address vulnerabilities in the organization's systems and networks;

Personal Liability Considerations

In a case of severe data breach, a CISO may not only lose the job, but can also be held personally liable when failing to report the data breach. In the US, a federal judge had fined a CISO and put him on 3-year probation for failing to report a data breach to the concerned regulatory agency.[9]

Such personal liability situations invariably arise when there is a deliberate attempt to cover up the breach. So, it is very important that the CISO must not only establish a clear process but also ensure that prescribed actions are taken for reporting every significant data breach as required by the law. As discussed earlier, CISOs must familiarize themselves with the CERT-In requirements for reporting a cybersecurity incident.

8 See: https://www.itarian.com/byod-bring-your-own-device/, last accessed on April 18, 2023.

9 See: Wall Street Journal (2023, May 3) "Former Uber Security Chief to Be Sentenced for Federal Crimes" https://www.wsj.com/articles/former-uber-security-chief-to-be-sentenced-for-federal-crimes-1b16114b, last accessed on May 23, 2023.

The Way Forward

With the Digital India Act set to replace the IT Act, it is possible that a wider range of cybercrimes will be defined. More effective steps to avoid and address incidents should be brought in, since one of the biggest criticisms of the IT Act has been the sheer lack of enforcement. Other new age issues such as payment of ransom for ransomware attacks would also need to be addressed. For e.g., the UK government has clarified that it does not consider payment of ransom as a reasonable step to safeguard data, and does not encourage such payments. The Federal Bureau of Investigation of the US also does not support such payments. Payment of ransomware may even be deemed illegal in the US if the payment is made to sanctioned countries, designated individuals or terrorists.

Due to rapid strides in digitalisation and technology adoption across the public and private sector, India has become a massive market engaged in both, (i) the research, development, and manufacturing of software products; as well as (ii) the sale of software products.[1] While the government and private sector have taken efforts to strengthen their cybersecurity measures, there is still much to be done. One potential solution lies in fostering greater public-private partnerships ("**PPPs**") in the cybersecurity domain. Collaboration between the government and private sector can help to leverage each other's strengths and expertise, leading to formulation of more effective cybersecurity measures.

A new, updated national cybersecurity policy is also the need of the hour. The policy should not only provide for education of people at all levels (including small cities and towns), but also provide for similar training requirements for enterprises. Security standards should be provided for enterprises to implement, with flexibility on the capability of smaller entities. Various sectors may come up with their own security standards since the type of data handled is different for different industries. On the other hand, the obligations under the Directions contain both vague and onerous requirements and based on the experience of the industry since June 2022, a fresh round of consultation should be held to revisit these requirements. While cybersecurity is a crucial goal for the country as a whole, regulations should not be so onerous so as to discourage compliance.

The Government of India has also initiated the Make in India policy which aims to promote the development, production, and assembly of products in India by Indian and international companies, with the aim of making the country a global hub for design and manufacturing. In furtherance of this policy objective, the Department of Industrial Policy and Promotion of the Ministry of Commerce and Industry has issued the Public Procurement (Preference to Make in India), Order 2017[2] (*modified by revision orders dated June 04, 2020*[3]*, and September 16, 2020*[4]).[5]

1 See: https://indianexpress.com/article/business/economy/dont-want-to-be-just-fuel-for-global-it-cos-want-ipr-platforms-in-india-7793774/, last accessed on May 05, 2023.

2 See: https://dpiit.gov.in/sites/default/files/publicProcurement_MakeinIndia_15June2017.pdf, last accessed on May 10, 2023.

3 See: https://dpiit.gov.in/sites/default/files/PPP%20MII%20Order%20dated%204th%20June%202020.pdf, last accessed on May 10, 2023.

4 See: https://www.meity.gov.in/writereaddata/files/PPP_MII_Order_dated_16_09_2020.pdf, last accessed on May 10, 2023.

5 To read further, please See: our hotline: https://www.nishithdesai.com/SectionCategory/33/Technology-Law-Analysis/12/60/TechnologyLawAnalysis/6230/1.html

Annexure A

Types of cybersecurity incidents mandatorily to be reported by Entities to CERT-In as per Annexure I to the Directions

A	Targeted scanning / probing of critical networks / systems
B	Compromise of critical systems / information
C	Unauthorised access of IT systems / data
D	Defacement of website or intrusion into a website and unauthorised changes such as inserting malicious code, links to external websites etc.
E	Malicious code attacks such as spreading of virus / worm / Trojan / Bots / Spyware /Ransomware / Crypto-miners
F	Attack on servers such as Database, Mail and DNS and network devices such as Routers
G	Identity Theft, spoofing and phishing attacks
H	Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks
I	Attacks on Critical infrastructure, SCADA and operational technology systems and Wireless networks
J	Attacks on Application such as E-Governance, E-Commerce etc.
K	Data Breach
L	Data Leak
M	Attacks on Internet of Things (IoT) devices and associated systems, networks, software, servers
N	Attacks or incident affecting Digital Payment systems
O	Attacks through Malicious mobile Apps
P	Fake mobile Apps
Q	Unauthorised access to social media accounts
R	Attacks or malicious / suspicious activities affecting Cloud computing systems / servers / software / applications
S	Attacks or malicious/suspicious activities affecting systems / servers / networks / software / applications related to Big Data, Block chain, virtual assets, virtual asset exchanges, custodian wallets, Robotics, 3D and 4D Printing, additive manufacturing, Drones
T	Attacks or malicious / suspicious activities affecting systems / servers/software / applications related to Artificial Intelligence and Machine Learning

concierge@nishithdesai.com

About NDA

At Nishith Desai Associates, we have earned the reputation of being Asia's most Innovative Law Firm — and the go-to specialists for companies around the world, looking to conduct businesses in India and for Indian companies considering business expansion abroad. In fact, we have conceptualized and created a state-of-the-art Blue Sky Thinking and Research Campus, Imaginarium Aligunjan, an international institution dedicated to designing a premeditated future with an embedded strategic foresight capability.

We are a research and strategy driven international firm with offices in Mumbai, Palo Alto (Silicon Valley), Bengaluru, Singapore, New Delhi, Munich, and New York. Our team comprises of specialists who provide strategic advice on legal, regulatory, and tax related matters in an integrated manner basis key insights carefully culled from the allied industries.

As an active participant in shaping India's regulatory environment, we at NDA, have the expertise and more importantly — the VISION — to navigate its complexities. Our ongoing endeavors in conducting and facilitating original research in emerging areas of law has helped us develop unparalleled proficiency to anticipate legal obstacles, mitigate potential risks and identify new opportunities for our clients on a global scale. Simply put, for conglomerates looking to conduct business in the subcontinent, NDA takes the uncertainty out of new frontiers.

As a firm of doyens, we pride ourselves in working with select clients within select verticals on complex matters. Our forte lies in providing innovative and strategic advice in futuristic areas of law such as those relating to Blockchain and virtual currencies, Internet of Things (IOT), Aviation, Artificial Intelligence, Privatization of Outer Space, Drones, Robotics, Virtual Reality, Ed-Tech, Med-Tech and Medical Devices and Nanotechnology with our key clientele comprising of marquee Fortune 500 corporations.

The firm has been consistently ranked as one of the Most Innovative Law Firms, across the globe. In fact, NDA has been the proud recipient of the Financial Times–RSG award 4 times in a row, (2014-2017) as the Most Innovative Indian Law Firm.

We are a trust based, non-hierarchical, democratic organization that leverages research and knowledge to deliver extraordinary value to our clients. Datum, our unique employer proposition has been developed into a global case study, aptly titled 'Management by Trust in a Democratic Enterprise,' published by John Wiley & Sons, USA.

Research@NDA

Research is the DNA of NDA. In early 1980s, our firm emerged from an extensive, and then pioneering, research by Nishith M. Desai on the taxation of cross-border transactions. The research book written by him provided the foundation for our international tax practice. Since then, we have relied upon research to be the cornerstone of our practice development. Today, research is fully ingrained in the firm's culture.

Over the years, we have produced some outstanding research papers, reports and articles. Almost on a daily basis, we analyze and offer our perspective on latest legal developments through our "Hotlines". These Hotlines provide immediate awareness and quick reference, and have been eagerly received. We also provide expanded commentary on issues through detailed articles for publication in newspapers and periodicals for dissemination to wider audience. Our NDA Labs dissect and analyze a published, distinctive legal transaction using multiple lenses and offer various perspectives, including some even overlooked by the executors of the transaction. We regularly write extensive research papers and disseminate them through our website. Our ThinkTank discourses on Taxation of eCommerce, Arbitration, and Direct Tax Code have been widely acknowledged.

As we continue to grow through our research-based approach, we now have established an exclusive four-acre, state-of-the-art research center, just a 45-minute ferry ride from Mumbai but in the middle of verdant hills of reclusive Alibaug-Raigadh district. Imaginarium AliGunjan is a platform for creative thinking; an apolitical ecosystem that connects multi-disciplinary threads of ideas, innovation and imagination. Designed to inspire 'blue sky' thinking, research, exploration and synthesis, reflections and communication, it aims to bring in wholeness — that leads to answers to the biggest challenges of our time and beyond. It seeks to be a bridge that connects the futuristic advancements of diverse disciplines. It offers a space, both virtually and literally, for integration and synthesis of knowhow and innovation from various streams and serves as a dais to internationally renowned professionals to share their expertise and experience with our associates and select clients.

We would love to hear from you about any suggestions you may have on our research publications.
Please feel free to contact us at **research@nishithdesai.com**.

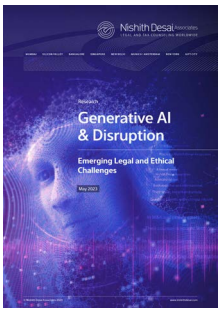
Recent Research Papers

Extensive knowledge gained through our original research is a source of our expertise.

May 2023

Sovereign Wealth Funds & Pension Funds: Investments into India

Regulatory, Legal and Tax Overview



May 2023

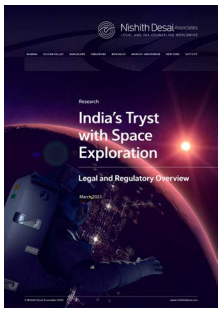
Generative AI & Disruption

Emerging Legal and Ethical Challenges

May 2023

M&A Lab

Adani's Hostile Takeover of NDTV



May 2023

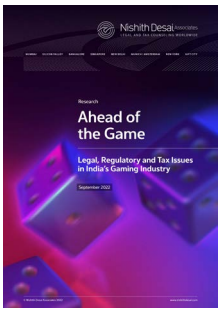
India's Tryst with Space Exploration

Legal and Regulatory Overview

January 2023

Doing Business in India

The Guide for US Businesses and Organizations Entering and Expanding into India



September 2022

Ahead of the Game

Legal, Regulatory and Tax Issues in India's Gaming Industry

For more research papers **click here**.

concierge@nishithdesai.com

Nishith Desai Associates

LEGAL AND TAX COUNSELING WORLDWIDE

MUMBAI

93 B, Mittal Court, Nariman Point
Mumbai 400 021, India

Tel +91 22 6669 5000

SILICON VALLEY

220 S California Ave., Suite 201
Palo Alto, California 94306, USA

Tel +1 650 325 7100

BENGALURU

Prestige Loka, G01, 7/1 Brunton Rd
Bengaluru 560 025, India

Tel +91 80 6693 5000

SINGAPORE

Level 24, CapitaGreen
138 Market St
Singapore 048 946

Tel +65 6550 9855

MUMBAI BKC

3, North Avenue, Maker Maxity
Bandra–Kurla Complex
Mumbai 400 051, India

Tel +91 22 6159 5000

NEW DELHI

13-H, Hansalaya Building, 15
Barakhamba Road, Connaught Place
New Delhi 110 001, India

Tel +91 11 4906 5000

MUNICH / AMSTERDAM

Maximilianstraße 13
80539 Munich, Germany

Tel +49 89 203 006 268

NEW YORK

1185 6th Avenue, Suite 326
New York, NY 10036, USA

Tel +1 212 464 7050

GIFT CITY

408, 4th Floor, Pragya Towers
GIFT City, Gandhinagar
Gujarat 382 355, India

Cybersecurity Law and Policy
Present Scenario and the Way Forward

concierge@nishithdesai.com