Report of the Working Group to study Cyber Liability Insurance

बीमा विनियामक और विकास प्राधिकरण
Insurance Regulatory and Development Authority of India

This page has been left blank

Dr. Subhash Chandra Khuntia
Chairman
Insurance Regulatory and Development Authority of India
Hyderabad

Respected Sir,

Subject: Working Group to study Cyber Liability Insurance – Submission of Report

We thank you for IRDAI order no. IRDAI/NL/ORD/MISC/260/10/2020 dated 19th October 2020 constituting a Working Group to study Cyber Liability Insurance.

We are pleased to submit the report of Working Group on the various terms of reference. The report is the culmination of collective efforts of the members of the working group and contributions of stakeholders.

On behalf of the members of the group and also on my behalf, we sincerely thank you for entrusting this responsibility. We sincerely thank all the executives of IRDAI for the cooperation and support they have extended to the working group. We also acknowledge with thanks inputs received from various stake holders.

Report on individual cyber insurance along with model policy wording has already been submitted on 23rd November, 2020

Yours Sincerely,

Place: Hyderabad
Date: 30-12-2020

P. Umesh
Chairman of the Working Group

Members
Ms. Kasturi Sengupta
Ms. Gisha George
Mr. Balaji Cuddapah
Mr. Parag Gupta
Mr. Ayush Jain
Mr. Segar Sampathkumar
Mr. A.R. Nithiyanantham
Mr. Dilip D. Dange

This page has been left blank

ACKNOWLEDGEMENTS

The Working Group is grateful to Dr. Subhash Chandra Khuntia, Chairman, Insurance Regulatory and Development Authority of India (IRDAI) for entrusting this task of great importance and providing an opportunity to study Cyber Liability Insurance, The Group is also thankful to Smt. T. L. Alamelu, Member (Non-Life) and Smt. Yegnapriya Bharath, Chief General Manager (Non-Life), Mr. K. Mahipal Reddy, General Manager for taking active interest in the deliberations of the Group and sharing their insights on the subject.

The Working Group, during its meetings on online platform of WebEx had interacted with representatives from various stakeholders and collected responses and deliberated extensively on the subject. The inputs offered by them proved to be immensely useful. The report is the culmination of collective efforts of the members of the working group and contributions of stakeholders.

The Working Group expresses sincere gratitude to the General Insurers carrying on Cyber Insurance Business for their valuable responses. The Working Group places on record its appreciation for and expresses gratitude to the invitees from insurers The New India, ICICI Lombard, HDFC Ergo and TATA AIG and Re-Insurers Swiss-Re, Munich Re, and Lloyds's India, General Insurance Council, Insurance Brokers Association of India, and industry experts for their active participation in the meetings and valuable contributions.

The Working Group expresses sincere gratitude to representatives of Tuli & Co, Solicitors & Advocates, Khaitan Legal Associates, Indian Advocates, Deloitte Touche Tohmatsu India LLP. IDRBT, Hyderabad Cyber Crime Police, CII, FICCI, NASSCOM/ DSCI, CERT-In and Ministry of Electronics &IT, for their active participation in the meetings and providing with useful insights into various aspects impacting cyber risk insurance.

The Working Group wishes to acknowledge the assistance and co-operation provided by IRDAI and its team in planning and organizing the various meetings of the Group. The detailed agenda notes, and minutes prepared by them for each of the meetings of the Group had enabled the Group to have meaningful and focused discussions. They had also immensely supported and contributed in preparation of this report.

The Working Group is grateful to the managements of IRDAI/Insurance companies/Re-Insurers and National Insurance Academy that the Working Group members represent for having spared the members with time and resources for completing this report.

P. Umesh
Chairman of the Working Group

भारतीय बीमा विनियामक और विकास प्राधिकरण
INSURANCE REGULATORY AND
DEVELOPMENT AUTHORITY OF INDIA

Ref: IRDAI/NL/ORD/MISC/260/10/2020 Dated: 16th October, 2020

ORDER

Re: Working Group to Study Cyber Liability Insurance

Amid the COVID 19 pandemic, there are rising incidences of cyberattacks and a growing number of high-profile data breaches. It is felt that cybersecurity is the most important need for all sectors today to address the numerous risks posed by cyber-attacks.

2 Since the online exposures offices, business organizations and other establishments face continue to increase even as they become more globally networked and complex, insurance products need to adapt to the changing environment. The General Liability policies do not cover cyber risks and cyber insurance policies currently available are highly customized for clients in a new and quickly growing market. Hence, it is felt that a basic standard product structure is required to provide insurance cover for individuals and establishments to manage their cyber risks.

3. To examine the need for standard Cyber Liability Insurance product, it has been decided to constitute the following Working Group.

i. Shri. P. Umesh, Consultant-Liability Insurance, Chair
ii. Smt. Kasturi Sengupta, Chief Manager, National Insurance Co. Ltd., Member
iii. Smt. Gisha George, Head - Liability Underwriting, Bajaj Allianz General Insurance Co Ltd, Member
iv. Shri. Balaji Cuddapah, President – Commercial SBU, Liberty General Insurance Ltd, Member
v. Shri. Parag Gupta, Chief Underwriting officer, Scor SE, Member
vi. Shri. Ayush Jain, Underwriter, Gen Re, Member
vii. Shri. Segar Sampathkumar, Chair Professor (General Insurance), National Insurance Academy, Member
viii. Shri. A.R. Nithiyanantham, Chief General Manager, IT Department, IRDAI, Member
ix. Shri. Dilip D. Dange,OSD(DGM), Non-Life Department, IRDAI, Member-Convener

4. The Terms of Reference of the Working Group are as follows.

a) To study various statutory provisions on Information and Cyber Security.
b) To evaluate critical issues involving legal aspects of transactions in cyber space.
c) To examine various types of incidents involving cyber security in the recent past and possible insurance coverage strategies for those.
d) To examine the cyber liability insurance covers available in Indian market and in other developed jurisdictions.
e) To recommend the scope of the cyber liability insurance covers for the present context and for the medium term.
f) To explore possibility of developing standard coverages, exclusions and optional extensions for various categories.
g) Any other matter relevant to the subject.

5. The Working Group may have its meetings through online mode and make its recommendations within two months of the date of this Order.

16/10/2020

(Yegnapriya Bharath)
Chief General Manager (NL)

Table of Contents

Item	Subject	Page No.
	Executive summary	1
	Introduction	7
Chapter 1	Various statutory provisions on Information and Cyber Security	11
Chapter 2	Critical issues involving legal aspects of transactions in cyber space	25
Chapter 3	Various types of incidents involving cyber security in the recent past and possible insurance coverage strategies for those	29
Chapter 4	Cyber liability insurance covers available in Indian market and in other developed jurisdictions	39
Chapter 5	Recommendation of the scope of the cyber liability insurance covers for the present context and for the medium term	51
Chapter 6	Exploring possibility of developing standard coverages, exclusions, and optional extensions for various categories	59
Chapter 7	Other Matters of Relevance	71
	Summary of views from various stakeholders	75
	References	83

This page has been left blank

EXECUTIVE SUMMARY

We live in a digital world today, and this world is teeming with innumerable risks of the known and unknown kind. Concurrent with the development of technology and digitally enabled possibilities for growth, data protection is emerging as a key concern. Globally, data protection has acquired salience. Data privacy and the need to secure the data a person holds is now recognised as an important responsibility. The insurance industry has been responsive in addressing the insurance needs in this space. But the coverage could be disparate, and the coverage terms could be onerous, which is understandable, given the shifting nature of the risk itself. The insurance industry is also impeded by lack of data on past losses, lack of clarity on the extent of their assumed risks under such coverage besides actuarial and underwriting challenges.

It is in this context that Insurance Regulatory and Development Authority of India (IRDAI) constituted a Working Group to Study Cyber Liability Insurance. The Working Group had detailed discussions with several stakeholders of the industry which included insurers, reinsurers, intermediaries, industry bodies, technology institutions and law firms. The Group members also had elaborated internal deliberations, and this Report presents the observations and recommendations of this Group.

Various Statutory Provisions on Information and Cyber Security:

It is necessary to understand the various statutory provisions governing cyber security in the context of cyber insurance, because these have a direct bearing on the cyber exposures necessitating insurance coverage. The report discusses the legal framework for Cyber Security consisting of Information Technology Act, 2000 (IT Act) and other statutes such as the Indian Penal Code, Indian Evidence Act, Bankers' Book Evidence Act, RBI Act and other sectoral provisions are also relevant.

With the enactment of the IT Act, India became the twelfth country to enact cyber laws in accordance with the United Nations endorsed model law. The Act dwells upon diverse aspects of cyber transactions. The provisions relating to offences such as unauthorised access, unauthorised extraction, Computer Virus, Disruption, Denial of Service, Destruction, Denial and Alteration are very relevant to Cyber Insurance. And of utmost significance is Section 43 A which deals with compensation for failure to protect data. This provision states that where a body corporate possessing sensitive personal data is negligent in implementing and maintaining reasonable security practices and thereby causes wrongful loss or wrongful gain to any person, such body corporate shall be liable to pay damages by way of compensation to the person so affected.

Personal Data Protection Bill, 2019 is also a very important piece of legislation which is currently being examined by a Joint Parliamentary Committee. The Bill is largely modelled on the European Union's General Data Protection Regulation and aims to protect the informational privacy of individuals by creating a preventive framework that regulates how businesses collect and use personal data.

Cyber laws of other countries were also studied by the Working Group and the legal framework on cyber security in United States of America, European Union and Singapore are discussed in the Report.

Critical Issues involving legal aspects of transactions:

Cyber law becomes important because it touches almost all transactions and activities involving the computer and internet. Every action and reaction in cyberspace have some legal and cyber legal angles.

- One of the most troubling issues in law relating to cyber space is jurisdiction. Jurisdiction in cyber space is clouded by the fact that parties involved in a transaction could be located across the globe and connected only virtually. There are no clearly defined geographical or jurisdictional boundaries in cyber space. A single cyber transaction could involve multiple laws of multiple parties engaged in the transaction.

- The IT Act does not lay down any requirement to inform the data subject of a cyber security incident. However, the rules framed thereunder do require the intermediaries to report cyber breaches to CERT-In, the national repository of cyber intrusion incidents. Sectoral Regulators too have laid down their own reporting requirements.

- Section 43 A of the IT Act provides remedies to persons affected by a cyber breach. These remedies have to be sought by initiating civil action against the negligent body corporate.

- Cybercrimes involving online payment transactions have become complex and have also significantly increased in scale. The sheer number of digital transactions involving banks and other payment entities and the need to provide real time, frictionless payment experiences to their customers leave these entities with very limited time to identify and respond to cyberthreats.

- Other critical issues include the challenges of identifying the cybercriminal as there are multiple layers between the perpetrator and the victim. Cyber laws involving multiple jurisdictions might not be uniform, and some of the provisions relating to specific incidents could even be conflicting with each other.

Cyber Security incidents and possible insurance coverage strategies:

A cybercrime involves computers and networks and includes a wide range of activities from the trivial to the tragic. The economic consequences of these attacks could be very serious for business and result in reputation damage.

Various incidents that have occurred in the past are discussed in this Report, along with the possible coverage provisions that would have mitigated some of the financial consequences of these incidents. The coverage provisions include:

- Meeting the cost of Notification
- Forensic Expenses
- Defence Costs
- Expenses incurred for dealing with the breach
- Extortion payment
- Public Relations costs
- Liability for customers
- Fines and penalties, where covered

In a globalized economy, exposures relating to notification requirements in other developed jurisdictions are important and the coverage offered needs to mitigate losses arising out of such exposures. Notification requirements in USA, EU and some other countries are mentioned in the report.

Cyber Liability covers available in India and other jurisdictions:

World over, the size of the cyber liability insurance market is quite small in comparison to other lines of business. Only a small fraction of the cyber losses is currently insured. Yet, the demand for cyber coverage has not acquired the sense of urgency that the exposures warrant. Many companies, be it in the service industry or in the manufacturing industry, do not yet appreciate the full magnitude of their cyber exposures and perhaps assume that traditional insurance lines would mitigate cyber losses. Even those industries which realise the scale and extent of their exposures, like the financial institutions, perceive cyber insurance coverage as too narrow or ambiguous to assure them of adequate recovery in the event of a loss.

On the supply side, Insurance Companies too, are treading cautiously, expanding their offerings at a conservative pace. Small coverage limits and high deductibles are characteristic of the cyber insurance coverage presently available. Reasons for such aversion could include limited actuarial data, the nature of unpredictable changes in the technology space, the radically changing patterns of use of technology and the terrifying capabilities of the perpetrators. These challenges are not only faced by Indian insurers, but globally too. Yet, as the world comes to terms with this new reality, insurers, corporates, and governments are working together to address them.

Even policies not designed to cover cyber related loses could ending up paying such claims by reason of Silent/ Non-affirmative covers. In the United Kingdom the Prudential Regulation Authority advised the insurance entities to address Silent Cyber issue. India too needs to address this issue.

The Report details the coverage available in the Indian and international markets. Some of the exposures for which coverage is not presently available in India are stated in the report.

Scope of Cyber Liability Cover for the immediate context and for medium term:

With the outbreak of the Covid 19 pandemic, the world has become more digital. Particularly in ecommerce, banking, and education there is a shift from the physical to the digital. This shift has also brought awareness on the dangers lurking in the cyber world.

MSMEs hitherto might not have realised the serious consequences of cyber exposures. But with the increasing digitisation of every human activity there is likely to be a change in their approach to cyber insurance. The enactment of Personal Data Protection legislation will also increase the need of the MSMEs for this coverage.

Cyber risks have no boundaries and permeate all classes of insurance. There is an urgent need to avoid assumption of unintended exposures through non-affirmative coverage. Some of the common market exclusions do not reflect current cyber realities and these may require immediate attention.

In the medium term, concurrent with the evolution of technology, and emerging needs of the market, new and additional coverage should become available. Recommendations are made for enhancements in the medium term that include cover for Bricking costs, unauthorised intrusion even though not targeted, Carveback for Bodily Injury and property Damage exclusion – to name a few.

The breadth and depth for these coverages would also depend upon the insurers' and reinsurers' view of the emerging exposures and loss experience.

Developing Standard terms for various categories:

The working group examined various aspects relating to cyber insurance in India including coverage issues, sector wise exposures, underwriting/ pricing methodology, and claims response and management to come to informed conclusion on standardisation.

The risk profiling and coverage design are expected to evolve over the next few years, concurrent with the evolution of legal landscape, technology, loss data base, risk evaluation and loss control practices. Given such sweeping changes happening in the cyber world, coverage terms have to respond speedily to the changing exposures.

The Working Group believes that early standardisation of cyber insurance in India, might impede innovation and hinder adaptation to evolving industry needs. It may lead to price-based competition instead of developing competencies for agility to design new products suitable to new environments.

While standardisation of Cyber insurance policy seems to be a very good approach, it presents many challenges. Cyber insurance is a response mechanism to cyber risks. Cyber risks are dynamic and evolving. Standardisation may not be able address all the emerging risks and is likely to limit innovation. Cyber insurance, at present, is much dependent upon support of reinsurers who instead of a standardised wording may prefer to use coverage and exclusions as per the latest developments in the market. Cyber insurance, being a relatively new product, calls for flexibility for gaining traction. However, there are certain aspects of cyber insurance that require a consensus and a common reference framework, and these terms are discussed in the Report.

Recommendations are also made on some issues relating to the scope of cover. Considering the evolutionary phase of cyber insurance, the recommendations are made for the immediate context and for medium term. To achieve the objective of clarity in coverage, the Group also suggests a Common Reference Framework for certain aspects of coverage.

Recommendations on scope of cover for the present context and medium term:

- Addressing silent cyber
- Comprehensive solutions
- Clarity on some payments – Fines & Penalties etc.
- Cover for Bricking costs

- Removal of Reference to Targeted Intrusion
- Carveback of cover under Bodily Injury and Property Damage exclusion
- Contingent Business Interruption
- Cyber Reputation loss
- Cover for Hardware Betterment costs
- Cover for Voluntary Shutdown following a Cyber Attack

Recommendations for common reference framework for clarity in coverage:

- Definition of Computer Systems
- Coverage for Fines & Penalties
- Intentional Acts exclusion
- Carveback of cover under Bodily Injury and Property damage exclusion
- Carveback of coverage for Cyber Terrorism
- Applicability of Failure to maintain Minimum Security Standards exclusion
- Changes in the risk

Report on individual cyber insurance along with model policy wording has already been submitted on 23rd November, 2020

INTRODUCTION

Humankind always faces risks from a multitude of elements, some of them unsettling, a few perplexing and a few more terrifying. However, Risk Management and Risk Transfer devices have always responded with effective solutions to manage risks and to mitigate their adverse consequences. The insurance industry has made a stellar contribution to progress with its agility in designing loss mitigation instruments.

The contribution of insurance industry is all the more profound, not just in loss mitigation, but in risk mitigation too. By its rigorous approach to risk analysis, risk evaluation, risk control, and risk reduction incentives, insurance has brought a significant awareness of risks and their consequences.

Particularly after Industrial Revolution, insurance industry has been ever receptive to the challenges of new exposures and has crafted many an innovative solution for loss mitigation. Not long ago, even an automobile was considered a dangerous chattel for the risks it posed to human safety. Third Party liability management has been one of the singular contributions that insurance industry can be proud of. Today, motor liability insurance policies are as ubiquitous as automobiles.

A similar threat has been wrought upon us by the Information Revolution. We live in a digital world today, and this world is teeming with innumerable risks of the known and unknown kind. While data is the new oil of the economy, just as oil could be inflammable and cause devastation, data, if not properly secured, could play havoc with the economy.

The proliferation of handheld devices, availability of internet access at affordable cost, increased computing power of mobiles, widening horizons of ecommerce, facilitation of payment gateways, the power of social media and its commercial possibilities and a multitude of such other factors are changing the way the world moves, works, sleeps, and conducts its business.

Now, not only execution, but even control functions are also done by digitally enabled machines. This has almost led to the subservience of mankind to machines. Every sphere of activity from manufacturing, finance, vehicular movement, aircraft navigation, distribution, weather prediction, education, health, and entertainment are dependent on a digital network of operations and control. The interdependence of these systems on each other amplifies the vulnerabilities. What makes cyber risks so potentially monstruous is the pervasive use of technology in every activity which was hitherto performed and controlled by humans. Cyber risks refer to the potential exposures to harm or loss or emanating from usage of information technology or systems.

India has been quick to seize the opportunities the digital realm offers. It has emerged as an Information Technology powerhouse. India is also one of the largest markets in the world, particularly with its young demography. The emergence of ecommerce, entertainment and financial ecosystems are opening new vistas of opportunities and, unfortunately, new trenches of threats.

The threats emanate from the dangers posed by accidental and deliberate breaches in the cyber space, which need to be fathomed and controlled.

Concurrent with the development of technology and digitally enabled possibilities for growth, data protection is emerging as a key concern. Globally, data protection has acquired salience. Data privacy and the need to secure the data a person holds is now recognised as an important responsibility. In India too, particularly after the Hon. Supreme Court recognised right to privacy as a fundamental right, data protection has become a major anxiety.

The legal framework for cyber liability is also evolving. Every person, be it an individual or an entity, is expected to exercise a duty of care to secure the data that he comes to possess, and to ensure that access to such data is not gained by unauthorised users. Should there be a breach in this duty, a cyber liability could arise. Regardless of whether the breach resulted in a financial loss to the person whose data is compromised, a breach of duty in cyber could result in grave legal and financial consequences. Notification and credit monitoring responsibilities, fines and penalties, and numerous other provisions make the responsibility of those who hold data onerous. One could never know what could be deemed to be reasonable care, what kind of threats could one foresee, and what kind of preventive measures one could have in place. Further, with most of areas of business operations getting automated and interconnected, vulnerability to disruption from cyber-attacks and resultant losses has increased significantly. There is a clear and present danger in the cyber world that cries out for a solution.

As ever, the insurance industry has been responsive in addressing these needs. Insurance solutions are indeed available for the risks faced by corporates and individuals. Undeterred by the uncertainties surrounding the evolution of cyber liability, the insurance industry has been quick to design risk and loss mitigation solutions in the form of cyber insurance. Cyber insurance is a form of insurance designed to protect an insured against damages caused by cyber risks. Cyber insurance is also referred to as cyber risk insurance, Cyber liability insurance, or Cybersecurity insurance.

But the coverage could be disparate, and the coverage terms could be onerous, which is understandable, given the shifting nature of the risk itself. The insurance industry is also impeded by lack of data on past losses, lack of clarity on the extent of their assumed risks under such coverage and other actuarial and underwriting challenges. Therefore, the exposures, the losses, and the coverage available to mitigate such losses need critical examination. Attempts also need to be made to develop a sound framework for loss assessment and mitigation, and to harmonise the efforts of the various risk carriers involved in this enterprise.

It is in this context that Insurance Regulatory and Development Authority of India (IRDAI) constituted a Working Group to examine the need for a Standard Cyber Liability Insurance Product. Mandated with this task, the Working Group deliberated upon the approach required to provide the needed insights. It was decided that the views of the major stakeholders be obtained in order to gain a good understanding of the cyber liability landscape.

Insurers, Reinsurers, Intermediaries, Industry Bodies, Technology Institutions and Law Firms were invited for virtual discussions with the Group. All of them actively participated in the discussions and provided valuable insights into the cyber ecosystem and its complexities, particularly in the context of cyber insurance.

The Working Group also studied the coverage for cyber exposures available within and outside the country and had detailed discussions on the various terms of reference.

This page has been left blank

Chapter -1
Various statutory provisions on Information and Cyber Security

Overview of Cyber Laws in India & other countries

India

The cyber law ecosystem in India comprises Information Technology Act, 2000 (IT Act) that came into force on 17th October 2000 and its further amendments, proposed Personal Data protection Bill 2019, Indian Penal Code, Indian Evidence Act, Bankers' Book Evidence Act , RBI Act and / or respective statute which may impact respective industry.

An overview of the various laws is elaborated as follows –

Information Technology Act, 2000 (IT Act)

When Information Technology Act 2000 was passed, India became the 12th country to enact cyber laws in accordance with UN-endorsed model law as the backbone of the cyber laws of different countries. Cyberlaw in India is not a separate legal framework. It is a combination of various laws. With the Computer and internet taking over every aspect of our life, there was a need for strong cyber laws. Cyber Laws provide legal recognition to electronic documents and a framework to support e-filing and e-commerce transactions and provides a legal framework to mitigate and check cybercrimes.

Information Technology Act, 2000 is India's mother legislation regulating the use of computers, computer systems and computer networks as also data and information in the electronic format. This legislation has touched varied aspects pertaining to electronic authentication, digital (electronic) signatures, cybercrimes and liability of network service providers.

The primary objectives of the IT Act are as under:

- Granting legal recognition to all transactions done through electronic data exchange
- Legal recognition of books of accounts in electronic form
- Addressing Computer-related crimes and cyber offenses
- Protecting privacy and sensitive personal data

The IT Act broadly covers the following entities within its ambit –

- Intermediaries

- Body Corporates

The rules under IT Act applicable to above entities are –

The Information Technology (Intermediaries guidelines) Rules, 2011: These rules provide the rights and responsibilities of internet intermediaries in India. If the Internet intermediaries follow these rules and exercise proper cyber due diligence, they are entitled to a "safe harbour protection". Otherwise, they are liable for various acts or omission occurring at their respective platforms once the matter has been brought to their notice. IT Act defines an intermediary as under:

Sec 2(W): "intermediary", with respect to any particular electronic records, means any person who on behalf of another person receives, stores or transmits that record or provides any service with respect to that record and includes telecom service providers, network service providers, internet service providers, web-hosting service providers, search engines, online payment sites, online-auction sites, online-market places and cyber cafes

The Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011: These rules, regarding sensitive personal data or information, are applicable to the body corporate or any person located within India. It basically, requires entities holding sensitive personal information of users to maintain certain specified security standards.

Provisions relating to Offences & Penalties

Some of the provisions relating to penalties and offences which are relevant in the context of general insurance are given below –

Section 43: Penalty and compensation for damage to computer, computer system, etc.– If any person without permission of the owner or any other person who is in charge of a computer, computer system or computer network –

a) accesses or secures access to such computer, computer system or computer network or computer resource;

b) downloads, copies or extracts any data, computer data base or information from such computer, computer system or computer network including information or data held or stored in any removable storage medium;

c) introduces or causes to be introduced any computer contaminant or computer virus into any computer, computer system or computer network;

d) damages or causes to be damaged any computer, computer system or computer network, data, computer data base or any other programmes residing in such computer, computer system or computer network;

e) disrupts or causes disruption of any computer, computer system or computer network;

f) denies or causes the denial of access to any person authorised to access any computer, computer system or computer network by any means;

g) provides any assistance to any person to facilitate access to a computer, computer system or computer network in contravention of the provisions of this Act, rules or regulations made thereunder;

h) charges the services availed of by a person to the account of another person by tampering with or manipulating any computer, computer system, or computer network;

i) destroys, deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means;

j) steal, conceal, destroys or alters or causes any person to steal, conceal, destroy or alter any computer source code used for a computer resource with an intention to cause damage;

he shall be liable to pay damages by way of compensation to the person so affected.

Section 43 A - Compensation for failure to protect data:

Where a body corporate, possessing, dealing or handling any sensitive personal data or information in a computer resource which it owns, controls or operates, is negligent in implementing and maintaining reasonable security practices and procedures and thereby causes wrongful loss or wrongful gain to any person, such body corporate shall be liable to pay damages by way of compensation to the person so affected.

("body corporate" means any company and includes a firm, sole proprietorship or other association of individuals engaged in commercial or professional activities)

Section 66 - Computer related offenses:

If any person, dishonestly or fraudulently, does any act referred to in section 43 (as explained above a to j), he shall be punishable with imprisonment for a term which may extend to three years or with fine which may extend to five lakh rupees or with both.

Explanation – For the purposes of this section -

a) the word “dishonestly” shall have the meaning assigned to it in section 24 of the Indian Penal Code;

b) the word “fraudulently” shall have the meaning assigned to it in section 25 of the Indian Penal Code.

Section 66 B - Whoever dishonestly received or retains any stolen computer resource or communication device knowing or having reason to believe the same to be stolen computer resource or communication device, shall be punished with imprisonment of either description for a term which may extend to three years or with fine which may extend to rupees one lakh or with both

Section 66C - Whoever, fraudulently or dishonestly make use of the electronic signature, password or any other unique identification feature of any other person, shall be punished with imprisonment of either description for a term which may extend to three years and shall also be liable to fine with may extend to rupees one lakh.

Section 66D - Whoever, by means for any communication device or computer resource cheats by personating, shall be punished with imprisonment of either description for a term which may extend to three years and shall also be liable to fine which may extend to one lakh rupee.

Some other relevant provisions are indicated below

Section 66E - Punishment for violation of privacy

Section 66 F - punishment (life imprisonment) for cyber terrorism

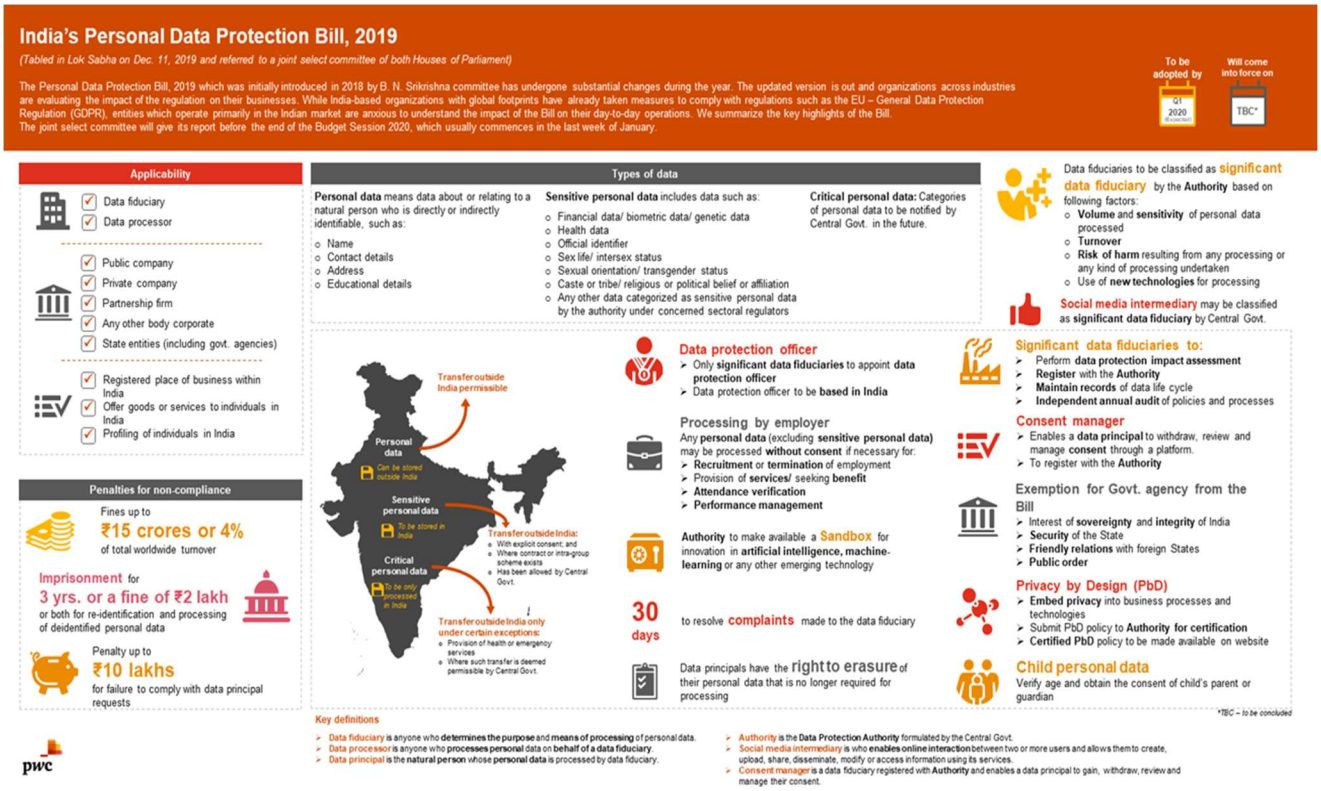
Section 67 / 67A / 67B - punishment for publishing or transmitting obscene material in electronic form

Section 72 - punishment (maximum of 2 years of imprisonment with fine of Rs 1 lakh) for disclosure of material without the consent of the person concerned to any other person

Section 72 A - punishment (maximum of 3 years of imprisonment with fine of Rs 5 lakhs) for disclosure of personal information in breach of lawful contract, to a third party

Personal Data Protection Bill, 2019:

This bill is largely modelled on the EU's General Data Protection Regulation (GDPR) and aims to protect the informational privacy of individuals by creating a preventive framework that regulates how businesses collect and use personal data. It is currently being examined by a Joint Parliamentary Committee in consultation with experts and stakeholders.



The Bill proposes to protect "**Personal Data"** relating to the identity, characteristics trait, attribute of a natural person and **"Sensitive Personal Data** such as financial data, health data, official identifier, sex life, sexual orientation, biometric data, genetic data, transgender status, intersex status, caste or tribe, religious or political beliefs.

The key stakeholders under the bill are:-

Data Principal - the natural person to whom the personal data relates

Data Fiduciary – any person, including the State, a company, any juristic entity or any individual who alone or in conjunction with others determines the purpose and means of processing of personal data;

Data Processor – any person, including the State, a company, any juristic entity or any individual, who processes personal data on behalf of a data fiduciary;

Key provisions

- Any entity collecting or using personal data should obtain consent from data principal. Processing of personal data should be done only for "clear, specific and lawful" purposes. Only that data which is necessary for such processing is to be collected from anyone.
- Processing of sensitive personal data should be based on "explicit consent" of the data principal.
- Critical personal data of Indian citizens should be processed in centers located within the country.
- Other personal data may be transferred outside the territory of India with some conditions. However, at least one copy of the data will need to be stored in India.
- In case of fiduciaries that are not present in India (e.g. Facebook, Google etc.), the law is applicable to one who carry out the business in India.
- The data fiduciary shall retain personal data only as long as may be reasonably necessary to satisfy the purpose for which it is processed.
- The right to be forgotten – It provides a data principal the right against the disclosure of their data when the processing of her personal data has become unlawful or unwanted.
- The right to confirmation and access allows individuals to find out what is being done with their data.
- Stringent norms for protecting the data of children, with a provision that companies be barred from certain types of data processing such as behavioral monitoring, tracking, targeted advertising and any other type of processing which is not in the best interest of the child.
- Every data fiduciary shall implement policies and measures to ensure that, managerial, organizational, business practices and technical systems are designed in a manner to anticipate, identify, and avoid harm to the data principal.
- The data fiduciary shall take reasonable steps to maintain transparency regarding its general practices related to processing personal data.
- Every data fiduciary and data processor shall undertake a review of its security safeguards periodically as may be specified and may take appropriate measures accordingly.

- The data fiduciary shall notify the Authority of any personal data breach relating to any personal data processed by the data fiduciary where such breach is likely to cause harm to any data principal.
- India does not have sector specific data protection legislation. But directives and guidelines are issued by sector regulators like RBI and IRDAI etc.
- While at present there is no central authority, The PDP Bill envisages the constitution of the Data Protection Authority of India ("DPAI") for enforcement of its provisions. Data protection laws apply to businesses established in other jurisdictions also to the extent provided in the respective legislations.

PDP Bill vs GDPR – Similarities & Divergences

Similarities	Divergences
Includes extraterritorial applicability	Broader scope of PDP Bill w.r.t definitions of PD & SPDI
Functionally similar concept of relevant parties	Introduction of consent managers
Rights of data principals	Vast difference in compliance requirements
Privacy by design policy	Extensive power to DPA under PDP Bill
Security safeguards	Age threshold for children and related compliances
Similar responsibilities of Data Protection Officer	NO SDF or registration of SDF under GDPR
	Non-EU controllers required to have a representative in EU
	Data transfer data localization
	No criminal penalty under GDPR
	Broad authority to Government under the PDP Bill
	Sandbox mechanism

Other laws

- The Indian Penal Code (as amended by the Information Technology Act) penalizes several cybercrimes. These include forgery of electronic records, cyber frauds, destroying electronic evidence, etc.

Identity thefts and associated cyber frauds attract the Indian Penal Code (IPC), 1860 – these can be invoked along with the Information Technology Act of 2000.

Relevant sections of IPC are:

Section 463 - Forgery
Section 464 - Making a False document
Section 468 - Forgery for the purpose of cheating
Section 469 - Reputation damage
Section 471 - Using a forged document as genuine

- Digital Evidence is to be collected and proven in court as per the provisions of the Indian Evidence Act (as amended by the Information Technology Act).

- In the case of bank records, the provisions of the Bankers' Book Evidence Act (as amended by the Information Technology Act) are relevant.

- Investigation and adjudication of cybercrimes is done in accordance with the provisions of the Code of Criminal Procedure, Civil Procedure Code, and the Information Technology Act.

- The Information Technology Act also amended the Reserve Bank of India Act paving the way for digital payments.

- Consumer Protection Act 2019 also makes reference to disclosure of personal information under Sec 2(47) Unfair Trade Practice as under: (ix) disclosing to other person any personal information given in confidence by the consumer unless such disclosure is made in accordance with the provisions of any law for the time being in force.

- Right to privacy is a facet of right to life and personal liberty enshrined under Article 21 of the Indian constitution and has been recognized as fundamental right in the recent judicial pronouncement by the Supreme Court in Justice K.S Putthaswamy v. Union of India.

- Besides the primary laws dealing with cybercrimes as mentioned earlier, there are sector-specific regulations issued by regulators such as the Reserve Bank of India (RBI), the Insurance Regulatory and Development Authority of India Act 1999 (IRDAI),the Department of Telecommunication (DOT) and the Securities Exchange Board of India (SEBI), that mandate cybersecurity standards to be maintained by

their regulated entities, such as banks, insurance companies, telecoms service providers and listed entities etc.

Other Countries

Furnished below is the listing of the provisions in information and cyber security and / or respective statute which may impact respective industry.

Region / Country	Law
European Union (EU) and the European Economic Area (EEA)	General Data Protection Regulation (GDPR)
USA	Identity Theft Act (18 U.S.C. 1028) Access Device Fraud Act (18 U.S.C. 1029) Computer Fraud and Abuse Act (18 U.S.C. 1030) Electronic Communications Protection Act ("ECPA"), Health Insurance Portability and Accountability Act (HIPAA) Gramm-Leach-Bliley Act, SEC Security Guidance
Singapore	Computer Misuse Act, Cybersecurity Act, Evidence Act, Enforcement of Personal Data Protection Commission (PDPC)

Some of the above acts are elaborated as below: -

European Union (EU) and the European Economic Area (EEA)

- The General Data Protection Regulation (GDPR) is a regulation on data protection and privacy for all individuals within the European Union (EU) and the European Economic Area (EEA). It also addresses the export of personal data outside the EU and EEA areas. This Regulation lays down rules relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data.

- The GDPR aims primarily to give control to individuals over their personal data and to simplify the regulatory environment for international business by unifying the regulation within the EU.

- The GDPR not only applies to organizations located within the EU but also applies to organizations located outside of the EU if they offer goods or services to, or monitor the behavior of, EU data subjects. It applies to all companies processing

and holding the personal data of data subjects residing in the European Union, regardless of the company's location.

- The GDPR was approved and adopted by the EU Parliament in April 2016. The regulation took effect from May 2018.

Important provisions from GDPR:

- **Personal Data:**
  Only if a processing of data concerns personal data, this regulation applies. Personal data are any information which is related to an identified or identifiable natural person.

- **Consent of data subject to use/process data:**
  Processing personal data is generally prohibited, unless it is expressly allowed by law, or the data subject has consented to the processing. Consent must be freely given, specific, informed and unambiguous. In order to obtain freely given consent, it must be given on a voluntary basis. The consent must be bound to one or several specified purposes which must then be sufficiently explained. Consent must be unambiguous, which means it requires either a statement or a clear affirmative act. The data subject shall have the right to withdraw his or her consent at any time.

- **Processing of personal data:**
  Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject, processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage.

- **Data protection officer:**
  The legal obligation to appoint a Data Protection Officer(DPO) is not the size of the company but the core processing activities which are defined as those essential to achieving the company's goals. If these core activities consist of processing sensitive personal data on a large scale or a form of data processing which is particularly far reaching for the rights of the data subjects, the company has to appoint a DPO.

  The duties of a Data Protection Officer include: Working towards the compliance with all relevant data protection laws, monitoring specific processes, such as data protection impact assessments, increasing employee awareness for data protection and training them accordingly, as well as collaborating with the supervisory authorities.

- **Direct marketing:**
  The data subject always has the right to object the processing of personal data for direct marketing purposes. If the data subject objects, the controller has to stop the processing for marketing purposes.

- **Encryption:**
  The Regulation places the responsibility on the controller and the processor to implement appropriate technical and organizational measures to secure personal data. The GDPR deliberately does not define which specific technical and organizational measures are considered suitable in each case, in order to accommodate individual factors. Encryption as a concept is explicitly mentioned as one possible technical and organizational measure to secure data.

- **Privacy impact assessment:**
  This refers to the obligation of the controller to conduct an impact assessment and to document it before starting the intended data processing. A data protection impact assessment must always be conducted when the processing could result in a high risk to the rights and freedoms of natural persons.

- **Records of processing activities:**
  GDPR obligates written documentation and overview of procedures by which personal data are processed. Records of processing activities must include significant information about data processing, including data categories, the group of data subjects, the purpose of the processing and the data recipients. This must be completely made available to authorities upon request.

- **The right of access:**
  The right of access includes information about the processing purposes, the categories of personal data processed, the recipients or categories of recipients, the planned duration of storage, information about the rights of the data subject. Information must be provided without undue delay but at latest within one month.

- **Right to be forgotten:**
  Personal data must be erased immediately where the data are no longer needed for their original processing purpose, or the data subject has withdrawn his consent and there is no other legal ground for processing, the data subject has objected and

there are no overriding legitimate grounds for the processing. In addition, data must naturally be erased if the processing itself was against the law in the first place.

- **Right to be informed:**
  GDPR gives individuals a right to be informed about the collection and use of their personal data, which leads to a variety of information obligations by the controller. Where data is obtained directly, the person must be immediately informed. The right to be informed also includes information about the duration of storage, the rights of the data subject, the ability to withdraw consent, the right to lodge a complaint with the authorities and whether the provision of personal data is a statutory or contractual requirement. In addition, the data subject must be informed of any automated decision-making activities.

- **Penalties for non-compliance:**
  Organizations can be fined up to 4% of annual global turnover for breaching GDPR or €20 Million. This is the maximum fine that can be imposed for the most serious infringements e.g. not having sufficient customer consent to process data or violating the core of Privacy by Design concepts. There is a tiered approach to fines e.g. a company can be fined 2% for not having their records in order not notifying the supervising authority and data subject about a breach or not conducting impact assessment. It is important to note that these rules apply to both controllers and processors.

United States of America

Being at the forefront of computer technology and the country that developed what is today referred to as the Internet, the USA has been the global leader in developing laws relating to cybercrime. While there are a few federal regulations, all the fifty states are free to have their own legislative authorities and there is no such rule that laws should be uniform or consistent.

Some of the relevant US laws are:

- Health Insurance Portability and Accountability Act (HIPAA): The HIPAA Privacy Rule provides federal protections for individually identifiable health information held by covered entities and their business associates and gives patients an array of rights with respect to that information.

- Gramm-Leach-Bliley Act: This Act requires financial institutions – companies offering consumers financial products or services like loans, financial or investment

advice, or insurance etc. to explain their information-sharing practices to their customers and to safeguard sensitive data.

- Computer Fraud and Abuse Act (18 U.S.C. 1030), which addresses fraud and related activity in connection with computers.

- Securities and Exchange Commission (SEC): SEC issued guidance to help issuers determine whether they needed to disclose certain cyber-vulnerabilities, past cyber-attacks, and other cyber security matters. In the recent past, it released a report summarizing best practices for securities market participants, including public companies, to monitor, assess, and manage their cybersecurity risk.

- California Consumer Privacy Act (CCPA): The California Consumer Privacy Act (CCPA) is a law that allows any California consumer to demand to see all the information a company has saved on them, as well as a full list of all the third parties that data is shared with. In addition, the California law allows consumers to sue companies if the privacy guidelines are violated, even if there is no breach. The law went into effect on January 1, 2020, but enforcement began on July 1. The CCPA includes two distinct categories of financial losses that could result from noncompliance: private right of action damages, either individually or as part of a class action, and regulatory fines and penalties.

- Federal Exchange Data Breach Notification Act of 2015: This bill requires a health insurance exchange to notify each individual whose personal information is known to have been acquired or accessed as a result of a breach of security of any system maintained by the exchange as soon as possible but not later than 60 days after discovery of the breach. A violation of this requirement is an unfair or deceptive act or practice under the Federal Trade Commission Act.

- Cybersecurity Information Sharing Act (CISA) 2015: It is enacted to create a voluntary cybersecurity information sharing process that will encourage public and private entities to share cyber threat information while protecting classified information, intelligence sources and methods, and privacy and civil liberties.

- Identity Theft Act (18 U.S.C. 1028), which addresses fraud and related activity in connection with identification documents, authentication features, and information and (18 U.S.C. 1028A) which addresses Aggravated Identity Theft.

- Access Device Fraud Act (18 U.S.C. 1029), which addresses fraud and related activity in connection with access devices.

- CAN-SPAM Act (18 U.S.C. 1037), which addresses fraud and related activity in connection with electronic mail.

- Communication Interference Act (18 U.S.C. 1362), which addresses interference to communication lines, stations, or systems.

Singapore

The Computer Misuse Act: It provides for penalty for several cybercrimes including unauthorized access to computer material, unauthorized modification of computer material, unauthorized use / interception of computer service, unauthorized disclosure of access code etc. It also provides for enhanced punishment for offences involving protected computers. The Criminal Procedure Code empowers a police officer to access a computer suspected of being used for criminal purposes.

The Cybersecurity Act: regulates owners of critical information infrastructure and regulates to cybersecurity service providers. It also authorizes measures to prevent, manage and respond to cybersecurity threats and incidents. The Cybersecurity (Critical Information Infrastructure) Regulations 2018 is also related to this issue. The Evidence Act was amended in 2012, to do away with outdated and cumbersome requirements for admitting computer output as evidence, and to replace these with presumptions regarding the authenticity of electronic records.

Enforcement of Personal Data Protection Commission (PDPC): to prevent the unauthorised disclosure of personal data. Bill to amend the PDPC in 2020 (to be confirmed):

- Fine minimum of SGD 1 million or 10% of turnover
- Notify PDPC within 3 days and individuals affected
- The organization must conduct assessment of suspected data breached

Chapter - 2
Critical issues involving legal aspects of transactions in cyber space

Cyber law becomes important because it touches almost all transactions and activities involving the computer and internet. Every action and reaction in cyberspace have some legal dimensions.

In today's techno-savvy environment, the world is becoming more and more digitally sophisticated and so are the crimes. Internet was initially developed as a research and information sharing tool in a relatively unregulated environment. With the passage of time, it became more transactional with e-business, e-commerce, e-governance, and e-procurement etc. All legal issues related to internet crime are dealt with through cyber laws. As the number of internet users is continuously on the rise, the need for cyber laws and their application gathered great momentum.

Some of the regular and well-known transactions in cyber space include:

- Online banking transactions/ Credit card & debit card transactions
- Ecommerce transactions
- Government forms/ returns in electronic form
- Digital signatures
- Data of all kinds stored in electronic form by various organizations
- Electronic communication using email, phones, and SMS
- Share transactions in DMAT form

Some of the critical issues involving legal aspects of transactions in cyber space are discussed below.

Jurisdiction

One of the vexing issues in the law relating to cyber space is Jurisdiction. Jurisdiction essentially refers to the concept where the power to determine and hear a case is vested with an appropriate Court in a legal system. The main issue that clouds Cyber Space Jurisdiction is the fact that parties involved in a dispute can be placed across the globe and are connected only virtually. The internet does not recognize any geographical or jurisdictional boundaries, but the users of the internet remain in physical jurisdictions around the world and are thus, subject to laws that are independent of their presence on the internet. A single internet transaction may involve laws of the country in which the user resides or the laws of the country that apply where the server hosting the transaction is

located or the laws of the country which apply to the person with whom the transaction takes place.

Digital Payments

With the rise of digital payments, cybercrimes involving payment transactions in the online space have significantly increased and become complex. While the RBI has been active in requiring companies operating payment systems to build secure authentication and transaction security mechanisms (such as 2FA authentication, EMV chips, PCI DSS compliance and tokenization), given that these payment companies often offer real-time frictionless payments experiences to their consumers, it leaves less time for banks and other entities operating in the payment ecosystem to identify and respond to cyberthreats. Hence, there is an increased need to identify and develop cybersecurity standards commensurate with the nature of information assets handled by them, and the possible harm in the event of any cybersecurity attack, to ensure that these emerging risks are mitigated.

Cyber Defamation

Cyber Defamation refers to publishing of false statement about an individual in cyberspace that can injure or demean the reputation of that individual. The ease of accessibility to and publication in online world has led to many cases of cyber defamation because of abuse of digital platforms by unscrupulous internet users. Added to this is the speed of travel of the message. While a person can be made liable for defamation both under civil and criminal laws in India, the challenge in this matter would be to identify the persons intending harm, as that person may not reveal his real name and identity in the cyber world.

Regulatory notification obligations

Cyber incidents can have repercussions both nationally and internationally. It is necessary that they are reported as soon as they are detected lest it might cause avoidable damage. Hence, there is a need for reporting them to appropriate authorities. In the Indian context, some provisions relating to reporting obligations are given below:

There is no specific requirement under the IT Act to inform the data subject of a cybersecurity incident. However, under the Intermediaries Guidelines, the intermediary is required to inform CERT-In of cybersecurity breaches. Further, specific types of cybersecurity incidents (target-scanning or probing of critical networks or systems, unauthorised access of an IT system and data, malicious code attacks, identity theft, spoofing, phishing, etc) have to be mandatorily reported to CERT-In by service providers, intermediaries, data centres and body corporates within a reasonable time of the occurrence of the incident to aid timely action.In addition, sector-specific regulators have

their own reporting requirements. For instance, the RBI requires banks to comply with the Cyber Security Framework in Banks, which, inter alia, requires banks to report cybersecurity incidents to the RBI within two to six hours.

Also, of interest and relevance would be the notification requirements in developed jurisdictions. Notification requirements imposed in many jurisdictions worldwide related to the release of personal information is given in box below:

Box 2.2. Notification and disclosure requirements and related fines and penalties

Data confidentiality breaches involving unauthorized access to personally identifiable information may be subject to notification and/or disclosure requirements (either to a regulator or to those affected) and fines and penalties in several countries:

- **In the United States**, there are prompt notification requirements established at the state- level in all but three states as well as federal privacy requirements that require notification (to regulators and affected individuals) if health or financial information is stolen (*Health Insurance Portability and Accountability Act* and *Graham-Leach-Bliley Act*, respectively). The requirements in 36 states as well as the federal requirements related to health information allow for the respective authorities to impose penalties on organizations for the release of that information. In addition, regulatory actions can be brought by a number of federal and state agencies, including the Federal Trade Commission and state Attorney Generals (Allianz Global Corporate & Specialty, 2015). The US Securities and Exchange Commission (SEC) requires disclosure by public companies of cyber incidents, where an incident is "reasonably likely to have a material effect on the registrant's results of operations, liquidity, or financial condition" and where an incident is likely to "materially affect a registrant's products, services, relationships with customers or suppliers, or competitive conditions" (SEC, 2011). Data breach incidents could be included within the scope of this disclosure requirement although a number of significant breaches have not been disclosed by public companies (Tsukayama, 2016).
- **In the European Union**, notification requirements are currently less prevalent although there are potential notification requirements in some sectors. The *Payment Services Directive 2*, for example, allows for the possibility of public ("payment service user") notification in cases where "an incident has or may have an impact on the financial interests of its payment service users". There are also notification requirements related to incidents that are operationally disruptive to critical services (see the section below on system malfunction). This will change as a result of the General Data Protection Regulation (GDPR) (*Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data*) which will come into effect in May 2018 and will include more generalized notification requirements. The GDPR will require prompt notification to the supervisor in cases where there is a risk to the "rights and freedoms of data subjects" (and to affected individuals if there is a high-risk) and will impose administrative fines in the case of breaches that are deemed intentional or involving negligence (Steptoe and Johnson LLP, 2016).
- **In Australia, Canada and Japan** fines may be imposed although only in the context of non-cooperation with an investigation or non-compliance with a specific order (BakerHostetler, 2015) (although, in Australia, changes to privacy legislation will lead to broad notification requirements and the potential for penalties of up to AUD 1.8 million for "serious or repeated interferences with the privacy of an individual" to be imposed by federal courts (Lui, 2017)). In Japan, financial sector businesses are required to notify the supervisory authority of data breaches while companies in other sectors may be required to notify supervisory authorities, depending on the nature of the data breach, the type of data involved and the number of data subjects affected, along with other relevant factors. In Singapore, the *Personal Data Protection Act* introduced requirements for the protection of personal data that is collected and fines of up to SGD 1 million can be imposed (Allianz Global Corporate & Specialty, 2015). An amendment to the Republic of Korea's *Personal Information Protection Act* allows for fines of up to KRW 100 million (and a prison sentence of up to ten years) (PwC, 2016). Mexico also imposes monetary penalties related to violations of the *Ley Federal de Protecci6n de Datos Personales en Posesi6n de Particulares* (Federal Law on the Protection of Personal Data held by Private Parties).

Redressal for unauthorised cyberactivity or failure to adequately protect systems and data

The IT Act makes statutory remedies available to persons affected. Section 43A of the IT Act expressly provides that whenever a body corporate possesses or deals with any sensitive personal data or information, and is negligent in maintaining reasonable security practices and procedures that in turn cause wrongful loss or wrongful gain to any person, the body corporate shall be liable to pay damages to the person affected. Therefore, the affected party may initiate a civil action against the negligent body corporate, making it liable to pay damages.

Other Legal aspects involved in certain cyber transactions

a) It is easy to identify individuals in the real world, but very difficult identify and reach a cybercrime suspect as most forms of online identification are complicated as there are multiple layers between the suspect and the victim. While with the advancement of technology, it is now possible to reach a suspect with all the forensics, it is yet not easy to take and enforce action because of various issues including issues of jurisdiction.

b) Many countries have cyber laws dealing with cybersecurity and cybercrimes. As provisions between laws of nations are not always the same and may contradict each other in some areas, there are bound to be issues with judicial outcomes for resolution of disputes in cyber transactions involving multiple jurisdictions.

c) Legality of Bitcoins & other Crypto Currency - Bitcoin, as a medium of payment, has neither been authorized nor been regulated by any central authority in India. There are yet no Cryptocurrency regulation in India.

d) Sanctions - Recently the US and EU issued sanctions against Cyber Hacking Groups, complicating the situation for victims of such attacks. Sanctions may now apply not only to the parties directly involved, but also the facilitators.

e) Fines and Penalties under GDPR and PDPB: Insurability of Fines and Penalties could become a moral issue and a matter of Public Policy This issue is particularly relevant in the context of insurance coverage. There is still ambiguity as to which penalties are payable, and which are not.

Chapter – 3
Various types of incidents involving cyber security in the recent past and possible insurance coverage strategies for those

Internet provides us with many tangible benefits- be it in communication, using search engines, doing financial transactions, availing online / web services, finding employment opportunities, finding life partner or even running entire businesses. Internet touches almost all aspects of our lives. However, it also makes individuals and enterprises, whether large or small, vulnerable to a wide range of threat actions from both internal and external threat actors.

A cybercrime is a crime involving computers and networks. This includes a wide range of activities, from illegally downloading music files to stealing money from online bank accounts etc. Cyber criminals are not always financially motivated. Cybercrimes include non-monetary offenses as well. It can include frauds such as job-related frauds, matrimonial frauds; stealing and misusing sensitive personal information (Aadhaar details, credit/debit card details, bank account credentials, etc.); defamation of an individual on social media, distribution of computer viruses etc.

New and powerful cyber-attacks are striking the internet at an alarming pace. A minor lapse in managing our digital lives can open the door to cyber criminals. Cyber criminals can steal our money or damage our reputation. According to a study by a leading industry research organization, 90% of all cyber-attacks are caused by human negligence. Therefore, cyber security awareness is important for everyone today. Over 313,000 cybersecurity incidents were reported in 2019 alone, according to the Indian Computer Emergency Response Team (CERT-In), the government agency responsible for tracking and responding to cybersecurity threats.

Whilst on the incidents involving cyber security, **The CRO Forum (2016)*** has developed a set of "incident type groups" that provides a useful categorisation of the different types of losses that could be incurred as a result of cyber incidents. The CRO Forum was formed in 2004 to advance risk management practice in the insurance industry. The CRO Forum member companies are large multi-national insurance companies. The members are headquartered across the world with a concentration in Europe.

The categories of losses put forward by the CRO Forum are described in Table below:

"Incident Type Group" (loss types)	"Coverage Scope"
Business interruption Interruption of operations	Reimbursement of lost profits caused by a production interruption not originating from physical damage.
Contingent business interruption (CBI) for non-physical damage	Reimbursement of the lost profits for the observed company caused by related third parties (supplier, partner, provider, customer) production interruption not originating from physical damage.
Data and software loss	Costs of reconstitution and/or replacement and/or restoration and/or reproduction of data and/or software which have been lost, corrupted, stolen, deleted, or encrypted
Financial theft and/or fraud	Pure financial losses arising from cyber internal or external malicious activity designed to commit fraud, theft of money or theft of other financial assets (e.g. shares). It covers both pure financial losses suffered by the observed company or by related third parties as a result of proven wrongdoing by the observed company.
Cyber ransom and extortion	Costs of expert handling for a ransom and/or extortion incident combined with the amount of the ransom payment (e.g. access to data is locked until ransom is paid).
Intellectual property theft	Loss of value of an intellectual property asset, resulting in pure financial loss.
Incident response costs	Compensation for crisis management/remediation actions requiring internal or external expert costs but excluding regulatory and legal defence costs. Coverage includes: (i) IT investigation and forensic analysis, excluding those directly related to regulatory and legal defences costs; (ii) public relations and communications costs; (iii) remediation costs (e.g. costs to delete or cost to activate a "flooding" of the harmful contents published against an insured); (iv) notification costs.
Breach of privacy [compensation]	Compensation costs after leakage of private and/or sensitive data, including credit-watch services, but excluding incident response costs.
Network security/security failure [liability]	Compensation costs for damages caused to third parties (supplier, partner, provider, customer) through the policyholder/observed company's IT network but excluding incident response costs. The policyholder/observed company may not have any damage but has been used as a vector or channel to reach a third party
Reputational damage (excluding legal protection)	Compensation for loss of profits due to a reduction of trade/clients because they lost confidence in the impacted company

Regulatory & legal defence costs (excluding fines and penalties)	A: Regulatory costs: compensation for costs incurred to the observed company or related third parties when responding to governmental or regulatory inquiries related to a cyber-attack (covers the legal, technical or IT forensic services directly related to regulatory inquiries but excludes Fines and Penalties). B: Legal defence costs: coverage for own defence costs incurred to the observed company or related third parties facing legal action in courts following a cyber-attack.
Fine and penalties	Compensation for fines and penalties imposed on the observed company. Insurance recoveries for these costs are provided only in jurisdictions where it is allowed.
Communication and media [liability]	Compensation costs due to misuse of communication media at the observed company resulting in defamation, libel, or slander of third parties including web-page defacement as well as patent/copyright infringement and trade secret misappropriation.
Legal protection - Lawyer fees	Costs of legal action brought by or against the policyholder including lawyer fees and costs in case of trial (e.g. identity theft, lawyer costs to prove the misuse of victim's identity).
Assistance coverage - psychological support Products [liability]	Assistance and psychological support to the victim after a cyber event leading to the circulation of prejudicial information on the policyholder without his/her consent. Compensation costs in case delivered products or operations by the observed company are defective or harmful resulting from a cyber event, excluding technical products or operations (Technology errors and omissions) and excluding Professional Services errors and omissions).
Directors and officers (D&O) [liability]	Compensation costs in case of claims made by a third party against the observed company directors and officers, including breach of trust or breach of duty resulting from cyber event.
Technology errors and omissions (E&O) [liability]	Compensation costs related to the failure in providing adequate technical service or technical products resulting from a cyber event.
Professional services errors and omissions (E&O)/Professional indemnity [liability]	Compensation costs related to the failure in providing adequate professional services or products resulting from a cyber event, excluding technical services and products (Technology errors and omissions).
Environmental damage	Coverage scope: compensation costs after leakage of toxic and/or polluting products consecutive to a cyber event.
Physical asset damage	Losses (including business interruption and contingent business interruption) related to the destruction of physical property of the observed company due to a cyber event at this company

Bodily injury and death	Compensation costs for bodily injury or consecutive death through the wrong-doing or negligence of the observed company or related third parties (e.g. sensitive data leakage leading to suicide).

Indian enterprises whether big or small are rapidly moving to the digital realm. There have been several cyber-attacks reported in India and around the world in the recent past. Economic consequences of cyber-attack can be immense to business and result into reputational damage

Appropriate covers under insurance policies can help mitigate losses resulting from the cyber-attacks. It may be noted that while of some these covers are available under traditional policies, stand-alone cyber insurance is becoming the ideal coverage instrument. Given below is the list of some of the incidents in the recent past with possible applicable covers.

Note: Information available in public domain only is mentioned here.

Company affected	**Description of the incident**	**Appliable Insurance Covers**
Dr Lal Path Labs data leak (October 2020)	Dr Lal Path Labs, one of the largest lab testing labs in India, kept the huge data of its patients on a public server unprotected for months. This has exposed the personal data of millions of patients in the public domain making it accessible to everyone last month. The lab testing giant serves around 70,000 patients a day. It was also among the few labs which got permission from apex health body ICMR to test Covid-19 patients	1) Defence costs and damages arising out of Privacy breach 2) Regulatory cost and fines 3) Consultant service cover including Forensics 4) Response cost incurred in making notifications to the affected person 5) Crisis Management Expenses Reference: https://www.the420.in/dr-lal-pathlabs-data-leak-fine-of-rs-5-crore-can-be-imposed-as-millions-of-patients-at-risk/
Haldiram's crucial data stolen	According to the FIR lodged, the cyber-attack took place on the intervening night of October 12	1) Consultant services expenses including Forensics

(October 2020)	and 13 and the hackers may have stolen "entire or substantial data" of the company which runs several restaurants and outlets. Hackers demanded INR 7.50 lakh to release information	2) Cyber extortion losses 3) Defence costs and damages arising out of data breach (in case if their client data has been stolen) 4) Response cost incurred in making notifications to the affected person Reference: https://www.business-standard.com/article/companies/haldiram-s-crucial-data-stolen-hackers-demand-rs-7-5-lakh-to-release-info-120101601338_1.html
Amazon hack (May 2019)	Amazon was the victim of a serious online attack by hackers who broke into about 100 seller accounts and funneled cash from loans or sales into their own bank accounts, according to a U.K. legal document. The hack took place between May 2018 and October 2018 Amazon found the accounts were likely compromised by phishing techniques that tricked sellers into giving up confidential login information.	1) Defence costs and damages due to Privacy and data breach 2) Consultant services expenses including Forensics 3) Response cost and Notification cost expenses including credit monitoring 4) Crisis management expenses Reference: https://www.financialexpress.com/industry/technology/amazon-hit-by-extensive-fraud-as-hackers-siphon-funds-from-100-seller-accounts/
Mondelez data breach (International - June 2017)	A global malware incident impacted the company's business. The malware affected a significant portion of the company's global Windows-	This claim was repudiated based on ground that the policy did not include a cover for a hostile or warlike action initiated by a government or sovereign power or

	based applications and its sales, distribution and financial networks across the company The company also incurred incremental expenses of $7.1 million because of the incident Mondelez made a claim for the costs on its property insurance policy that, it said, provided cover for "physical loss or damage to electronic data, programs, or software, including physical loss or damage caused by the malicious introduction of a machine code or instruction	any state-funded actor/s. This was contested by Insured and the matter is in a court of law in USA. Reference: https://www.cybersecurity-insiders.com/mondelez-files-100m-claim-from-zurich-insurance-for-notpetya-cyber-attack/
British Airways (September 2018)	On 6 September 2018, British Airways informed its customers that details from around 3,80,000 booking transactions had been stolen, including bank card numbers, expiry dates and cvv codes. It took the firm just one day to announce it had been hit by a cyber-attack between 21 August and 5 September. Soon afterwards, it was discovered the details were taken via a script designed to steal financial information by 'skimming' the payment page before it was submitted. Loosely translated, it appears that the hackers placed themselves in a position to read all of the data coming into BA's booking system, including	Defence costs and damages arising out of privacy breach 1) Consultant services expenses including Forensics 2) Crisis Response cost, credit monitoring expenses, notification cost to affected customers 3) Insurable Fines and Penalties 4) Regulatory costs Reference: https://www.pinsentmasons.com/out-law/news/british-airways-fined-20m-over-gdpr-breach

	customer's names, addresses, dates of birth, bank details and critically their CVV numbers. (According to the Payment Card Industry Data Security Standard (PCI DSS), which applies to companies accepting credit card information, storing CVV information is not allowed to be held on any company's data base as they are considered as such a vulnerable piece of information. Not only will British Airways face the bill for making good on all their customers potential losses, but they could also face a large fine. The latest GDPR regulations allows for a fine of up to 4% of worldwide turnover, and for a company that had turnover of £12 billion in 2017, this fine could be more than £480m)	
Big Basket user data for sale online (October 2020)	India's top online grocer Big basket has suffered a potential data breach resulting in personal information of over 20 Mn customers being allegedly sold on the dark web.	1) Defence costs and damages arising out of privacy breach 2) Consultant services expenses including Forensics 3) Notification cost. credit monitoring expenses, response cost 4) Crisis management expenses Reference:

		https://indianexpress.com/article/explained/explained-how-big-is-the-bigbasket-data-breach-7026688/
Unacademy learns lesson about security (May 2020)	Breach dates to January, hacker claims to have access to entire the database. Unacademy, one of the most popular online educational platforms in India, has suffered a major security breach that led to the exposure of data of around 20 million of its subscribers.	1) Defence costs and damages arising out of privacy breach 2) Notification cost, credit monitoring expenses, response cost 3) Consultant service cover including Forensics 4) Crisis management expenses Reference: https://www.theweek.in/news/sci-tech/2020/05/07/unacademy-hacked-data-of-20-mn-users-up-for-sale.html
Local search provider JustDial exposes data of 10 crore users (April 2019)	More than 10 crore users of local search service Justdial in India have been potentially affected by the data leaks, including their names, email ids, mobile number, gender, date of birth and so on were reportedly made public.	1) Defence costs and damages arising out of privacy breach 2) Notification cost, credit monitoring expenses, response cost 3) Consultant service cover including Forensics 4) Crisis management expenses Reference: https://www.timesnownews.com/business-economy/companies/article/justdial-data-breach-affects-more-than-10-crore-users/402297
Dr. Reddy's Laboratories Ltd.	Indian pharmaceutical company Dr. Reddy Laboratories reported a cyber-attack about a week after the company was granted	1) Defence costs and damages arising out of Privacy breach 2) Regulatory cost and fines

(October 26, 2020)	permission to begin its final stage trials for a Russian COVID-19 vaccine. In a statement to the National Stock Exchange of India, the company said it had isolated all data centers services and took required preventive actions.	3) Consultant service cover including Forensics 4) Response cost incurred in making notifications to relevant authorities Reference: https://www.scmagazine.com/home/security-news/dr-reddy-labs-discloses-cyberattack-soon-after-getting-ok-for-final-covid-vaccine-trial/
Mega Mumbai power outage (October 2020)	A malware attack is suspected to be the reason behind Mumbai's power outage last month. The case is being probed by the state's cyber department and the final report is awaited.	1) Consultant service cover including Forensics 2) Business interruption losses Reference: https://www.indiatoday.in/india/story/mumbai-power-outage-malware-attack-1742538-2020-11-20

This page has been left blank

Chapter - 4
Cyber liability insurance covers available in Indian market and in other developed jurisdictions

Cyber Insurance in India

Cyber insurance market in India and abroad is growing but it is still quite small compared to other insurance lines of business. Only a small fraction of cyber losses is currently insured. Still the demand for cyber coverage remains limited. Many companies be it in service industry or manufacturing industry do not yet appreciate the full extent of cyber risk, or they assume that traditional insurance lines will protect them. Others like financial institutions recognize the risk but see cyber insurance coverage as too narrow or ambiguous to guarantee adequate recovery at their hour of need.

Insurance companies on the other hand, are treading cautiously, expanding their offerings at a conservative pace. Most cyber insurers offer small coverage limits and high deductibles, and they may limit coverage in areas like business interruption, because cyber risk is difficult to estimate and price accurately. Further, there is too little actuarial data to draw upon. The risks at play evolve continuously based on unpredictable changes in digital technology itself, the radically changing patterns of technological use, hacker/perpetrators' capabilities / intentions etc.

These and other challenges of covering cyber risk are well-known in the insurance world globally. Internationally and in India, Insurers, insureds, and governments have worked steadily and incrementally to address them. Consequently, more cyber insurance coverage is being sold each year—including policies specifically created for cyber risk (known as "standalone" cyber coverage), as well as some traditional lines, like property and casualty insurance, that are revised to include cyber alongside other risks (adding a "cyber endorsement" to a broader policy).

Synopsis of Covers Available in Indian Market

Cyber insurance can be offered as a stand-alone product and as an add-on coverage to traditional lines of business. It can include coverage for both first party and third-party liabilities. Most insurers provide insurance solutions with appropriate endorsements and add on services as well and some insurers also offer their products through coinsurance and reinsurance with other insures due to capacity constraints.

The standard coverages currently available and normally offered in India in a stand-alone cyber insurance policy can be summarised as below:

First party Coverage	Third Party Liability Coverage	Coverage for other services
• Business interruption losses • Cyber Extortion • Theft of funds/ Loss of funds • Data restoration costs	• Privacy and Data Breach Liability including Customer notification and Credit Monitoring • Network Security Claims Cover • Multimedia / Media Liability Cover • Regulatory / Data administrative inquiry and insurable fines and penalties • E-payment Contractual Damages • Defence Costs	• Crisis management cover including public relations costs • Consultant Services Cover

As indicated, coverage for losses due to cyber incidents can be categorized by differentiating between losses borne as a direct result of the incident (first party coverage) and losses incurred as a result of litigation by alleged injured parties (third party coverage) and coverage for other services. As policy wordings vary from insurer to insurer, only major generic coverage features, exclusions and extensions are discussed here.

Coverage:

1. First Party Coverage:

a) **Business interruption:** Coverage is offered for business interruption loss (loss of net profits) as a result of a Cyber-attack that causes total or partial unavailability of the company's computer system which are in direct control of the insured. Coverage for such loss of profit is subject to waiting periods (in hours or days) as agreed in the policy. Further, costs incurred to restore the Company's Computer System to the same

level of functionality which existed immediately prior to such event and the costs to retrieve or reinstall Data or Computer Programmes are also offered.

Also, the costs associated with continuing to run the insured's business, including payroll expenses, as well as the costs associated with reducing the impact of the income loss (generally referred to as extra expenses) are also covered. Proof of loss is required by the insurer to quantify the losses claimed by the insured. In some instances, a forensic accountant may be called upon to perform a more thorough analysis to substantiate the extent of loss.

b) **Cyber Extortion:** Coverage is offered for Cyber Extortion Loss that the Insured incurs solely and directly as a result of a Cyber Extortion Threat.

Such loss is triggered when a hacker breaks into computer system and threatens to commit a wicked act like damaging the data, introducing a virus, initiating a denial of service attack, or releasing confidential data unless the insured pays a specified sum. Coverage typically extends to any extortion payment that the company has to make and expenses incurred while responding to the demand.

Cyber extortion can take various forms, but ransomware is by far the most common variant. Ransom ware is a type of malicious software that, when launched within a computer (usually from an e-mail opened by an unsuspecting employee), encrypts data or locks access to critical applications. An anonymous demand for payment then overlays the computer screen demanding payment, usually in bitcoin or any other currency—a form of electronic currency that is difficult to trace—in exchange for the decryption key.

Other forms of cyber extortion include denial-of-service attacks that disrupt networks until payment is made, or threats to disclose customer data or other confidential information unless a specific demand is met. Possible losses could be forensic cost, cost of consultant to negotiate with fraudsters and extortion money.

c) **Theft of Funds/ Loss of Funds Cover:** Coverage is offered for IT Theft Loss caused due to Funds wrongfully or erroneously paid by the Insured as a direct result of hacker's intrusion into the Company's Computer System which results in fraudulent and unauthorised deletion or alteration of Data contained in the Insured's Computer System. As a result of tampering within the insured computer systems, the insured ends up becoming inadvertent victim of fraudulent, dishonest, or malicious payment instructions and fund transfers.

This coverage could also extend to include loss sustained due to unauthorised communication triggered by insured's computer system to financial institutions, suppliers or such other third parties that lead to fraudulent fund transfers or financial transactions.

d) **Data Restoration Costs:** Coverage is offered to technically restore, retrieve or reinstall Data or Computer Programmes, including the cost of purchasing a software licence necessary to reproduce such Data or Computer Programmes which would have got lost or impacted during a cyber-attack incident.

2. Third Party Liability Coverage:

a) **Privacy and Data Breach Liability including customer notification and credit monitoring costs:** Coverage is offered for Damages and Defence Costs for a claim made against the Insured by any affected person or a client resulting from a privacy beach or a data breach for which the Insured is legally liable.

Sensitive, personal, or confidential third-party data that resides with the Insured could get compromised due to a cyber-event and could lead to third party claims for damages. Data breaches are characterized by (1) loss, theft, or unauthorized disclosure of personally identifiable information (PII) in company's care, custody, and control; (2) damage to data stored in the company's computer systems belonging to a third party; (3) transmission of malicious code or denial of service to a third party's computer system; (4) failure to timely disclose a data breach; (5) failure of the company to comply with its privacy policy prohibiting disclosure or sharing of PII; and (6) failure to administer an identity theft program required by governmental regulation or to take necessary actions to prevent identity theft. In addition, this clause covers the cost of defending claims associated with each of these circumstances.

Insured could also incur substantial Response costs that may include (i) notification expenses towards the affected third parties and regulators in such an event (ii) credit monitoring services for a defined period - these include the monitoring of one's credit history for a specified period for to detect any suspicious activity or unauthorized charges. It also may provide special alerts when there are noticeable changes to one's credit history (iii) cost of identifying and preserving relevant Data on the Company's Computer System

b) **Network Security Claims Cover:** Coverage is offered for Damages and Defence Costs arising from Third Party Claim against an Insured for any actual or alleged act,

error or omission of the Insured as a result of which a Cyber Attack would have occurred.

It covers claims against company for negligent acts, errors or omissions that result in a denial of service attack, unauthorized access, introduction of a virus, or other security breach of the Insured's computer system. This clause also offers cover for claims alleging company's failure to protect sensitive data stored in company's computer system.

c) **Multimedia / Media Liability Cover:** Coverage is offered for damages and Defence Costs arising from Third Party Claim made against an Insured for Media liability in context of Insured's publication or broadcasting of any digital media content.

This clause offers cover for lawsuits against company for acts like libel, slander, defamation, and copyright infringement, invasion of privacy or domain name infringement. These acts are covered only if they result from company's publication of electronic data on the Internet.

d) **Regulatory / Data administrative inquiry and insurable fines and penalties:** Coverage is offered for insurable fines and penalties and defence Costs arising from a Claim by a Regulator made against an Insured which arises out of a Data Breach or Privacy Breach.

It covers the costs of dealing with privacy regulatory authorities / agencies (which oversee data breach laws and regulations), including

- the costs of hiring lawyers to consult with regulators during investigations and
- the payment of regulatory fines and penalties (insurable by law) that are levied against the insured (as a result of the breach).

Data breaches typically involve customers residing in multiple countries and because each country has its own unique set of laws and rules, regulatory defence and penalties coverage is especially valuable given the need for company to deal with multiple sets of regulators.

e) **E-payment Contractual Damages:** Coverage is offered for Damages, Contractual Damages/Penalties and Defence costs arising from a Claim made against an Insured by a E-Payment Service Provider alleging a negligent breach of any published Payment Card Industry Data Security Standards that the Insured is required to comply with.

Companies engaging into contract with payment service providers may face serious actions from such service providers when the Insured fails to comply with payment card industry related regulations. Such losses could include defence costs, claim investigation costs, court awards and contractual penalties.

f) **Defence Costs:** Coverage is offered for expenses including the cost of hiring a lawyer, court fees, investigations, gathering facts, filing legal paperwork, and other related costs that the Insured may incur to defend itself from legal claims made by third parties like customers and regulators.

3. Services offered:

a) **Crisis management cover including public relations costs:** Coverage is offered for Public Relation Expenses incurred by the Insured to prevent or reduce the effects of negative publicity caused due to a cyber-attack event.

This provides cover for costs incurred for hiring a public relations consultant for managing the marketing and public relations for the Insured to protect their reputation following a cyber-attack event.

b) **Consultant Services Cover:** Coverage is offered for consultant costs incurred by the Insured:

- to prove the amount and the extent of a covered Loss and to investigate the source of such Loss and adequate steps to mitigate it.

- To prove that the Insured on the ground of facts reasonably suspects a Privacy Breach, Cyber Attack or Business Interruption Event, to investigate if and to what extend such Privacy Breach, Cyber Attack or Business Interruption Event has taken place, the causes of such event and how it can be mitigated.

IT and forensic expert costs incurred to investigate cyber-attack related events are covered. Such costs are integral to the policy coverage as cyber claims are quite complex and significant IT and forensic efforts are required to manage and quantify the effect and extent of a cyber loss.

Extensions:

1) **Cover for Cyber Terrorism - Coverage for claims emanating from or perpetrated by cyber terrorists:**
   Cyberterrorism is the use of the Internet to conduct violent acts that result in, or threaten, loss of life or significant bodily harm, in order to achieve political or ideological gains through threat or intimidation. Companies could become victims of such disruptive Internet activities and incur first party and third-party losses.

2) **Reward Expenses:** Reward Expenses offered by the Insurer for information that leads to the arrest and conviction of any individual(s) committing or trying to commit any illegal act. This extension offers cover for the amount that an Insured pays to an Informant for information not otherwise available which leads to the arrest and conviction of persons responsible for a Cyber-attack, Fraudulent Access or Transmission, or a Threat.

3) **Psychological Support expenses:** This extension covers all reasonable expenses for any trauma or distress caused to a stakeholder of the Insured because of a cyber-attack. Cyber situations can potentially cause psychological distress to the persons involved in the crisis. This extension offers cover for counseling expenses incurred by such affected parties.

4) **PCI DSS Assessment cover / E-payment Cost:** Coverage for any written demand received by an Insured from a Card Association or Acquiring Bank imposing assessment costs. Company's negligent breach of published card industry regulations may be exposed to claims by E-Payment Service Provider for damages. Losses could include defence cost, contractual penalties, and court awards.
5) **Social Engineering coverage:** Comprehensive cover for loss arising from impersonation of critical stakeholders that are acted upon based on good faith by the insured. Companies could become victims of third party's fraudulent electronic payment communications as fraudulent or dishonest impersonation of a company's Director, CEO, CFO. This may result into direct loss of funds.

Major Exclusions:

1) **Dishonest or Deliberate Wilful conduct**

   Any fraudulent, dishonest activity, willful violation, breach of law done by the insured stands excluded from scope of coverage. This exclusion could be amended to include

defence cost coverage for innocent insured and could also contain final adjudication clause.

2) **Contingent Business Interruption**

This clause excludes any business interruption loss resulting from damage to the computer system of a service provider or a supplier on which the insured depends.

3) **External Infrastructure Failure**

This clause excludes any claims arising due to any electrical or mechanical failure of infrastructure including any electrical power interruption, surge , brown out , black out , failure of telephone lines , data transmission lines , any satellite failure or any other telecom / network infrastructure which are not under the control of the insured / the outsource service provider.

4) **Bodily Injury and Property Damage**

This clause excludes any actual or alleged bodily injury, sickness, mental anguish or emotional distress or disturbance, disease or death of any person howsoever caused or damage to or destruction of any tangible property, including loss of use thereof. As the control and operation of physical assets becomes increasingly managed by computers that are themselves interconnected, cyber-attack on automation / operational technologies could cause property damage and bodily injury related losses. Such losses are excluded from cyber policy as the Property and casualty policies are expected to address coverage for bodily injury and property damage. Insurers may consider extending the coverage by amending the definition of Bodily Injury to include mental anguish, mental injury, emotional distress resulting from a Privacy Breach or Media Wrongful Act.

5) **War, terrorism, Invasion, riot, or insurrection**

This clause excludes coverage for loss from acts of war, terrorism, invasion, and/or insurrection. Since the repercussions of state-sponsored, political, and ideological cyber-attacks could be too vast and across industries, coverage for such events is excluded.

For ex. NotPetya exposed a serious ambiguity in how insurance policies treat state-sponsored cyber incidents. Some property and casualty insurers declined to pay NotPetya-related claims, invoking their war exclusions.

However, recently there is coverage available for “cyberterrorism” or “electronic terrorism”, but Cyber war still stays as a common exclusion.

6) **Monetary and Trading losses**

The theft of money, trading losses or securities are typically excluded from a cyber-policy.

7) **Prior act**

Cyber policies typically exclude any cyber incidents which existed prior to the insurance policy commencement.

8) **Unauthorized collection of data and Unsolicited Communication**

This clause excludes any unlawful or unauthorized collection of data and distribution of unsolicited correspondence or communications (whether in physical or electronic form), wiretapping, audio or video recordings or telephone marketing.

9) **Contractual Liability/ Assumed liability**

The policy excludes any liability under any contract, agreement, guarantee or warranty assumed or accepted by an Insured except to the extent that such liability would have attached to an Insured in the absence of such contract, agreement, guarantee or warranty

Study on the Cyber Insurance in other Jurisdictions including USA

The USA is the largest market and is estimated to account for the 90% of the Global standalone Cyber premium. It has been the main contributor behind the growth of cyber premium. The impressive growth rates in their cyber markets have been driven by several factors like

- Data breach legislation was progressively enforced in almost all the states in the USA (Alabama and South Dakota are the only ones without a statute) Mandatory Data Breach disclosure law was first signed in 2002 in California making firms legally obliged to notify affected parties in the event of data breach. Similar legislations were subsequently enforced in other states between 2005 to 2016.

- A rising awareness on Cyber threats involving large corporations targeted by hacking groups like Sony in 2011, Target in 2014, E-Bay in 2014 and Yahoo breaches of 2013-14 disclosed in 2016 etc.

The U.S. market is much more developed than its European counterpart, partly because the U.S. have had reporting requirements for cyber-attacks in place for several years with

relatively heavy fines for violations. These regulations have considerably increased the awareness of cyber risk and increased the demand especially for liability (third party) cyber coverage. The U.S. market is thus mainly dominated by third party coverage, whereas in Europe focus more on first party coverage. However, GDPR in the EU has become an important driver in the development of the European cyber insurance market.

On a comparison of the policy coverage in India with the global policy offerings, it is observed that the following covers which are available globally, are not available in India currently in the normal course or offered by few insurers selectively. The reasons are not difficult to understand as cyber insurance is in a nascent stage in India.

Bricking costs: Cyber products usually cover costs to replace / restore / recreate data and software that have been destroyed, corrupted or damaged and not the Computer System itself (computer, server, mobile phones, Industrial control systems, etc.) using / storing such data or software. Purpose of this extension is to cover replacement costs for such equipment that is rendered useless for its intended purpose because of a Security Incident or a System Failure ("bricking").

Coverage for Hardware Betterment costs: These include digital asset replacement costs the insured incurs due to the alteration, modification, deletion, denial of access to, damage, corruption or destruction of digital assets. Hardware betterment expenses include increased memory capacity or processing speed necessary to install more secured IT system standard technological advances. These may be necessary to prevent the re-occurrence of alteration, modification, deletion, denial of access to, damage, corruption or destruction of digital assets caused by a cyber-attack.

Crypto Currency Payments: Cyber Extortion loss which provides coverage for payment in Digital Currency including Crypto Currency particularly for payment in respect of extortion payments. As on date, there is no clarity on the legality of crypto currency payments in India.

Consumer Redress Fund: This provides coverage for payment which the Insured is legally required to pay, or has agreed to pay by way of settlement, to establish a fund for the payment of consumer claims. This may include fines and penalties which the insured's customer may be required to pay because of a security incident or data breach attributable to the insured

Contingent Business Interruption: The objective here is reduce the impact of the events outside the control of Insured. It covers business interruption loss and expenses incurred as a result of an interruption, degradation of service or unplanned suspension of a supplier / receiver Computer System. It creates exposure to third party IT systems which are

commonly used as entry point for cyber-attacks. The cyber contingent business interruption risk of an insured single company is characterised by the exposure and the information security level of the relevant provider of IT services or of the suppliers of goods. There are insured organisations which represent a higher exposure than others by virtue of their industry sector. For example, there is an above average dependence on IT services by retailers, financial institutions, and IT service providers themselves, as well as by organisations active in the tourism, hospitality, logistics and transportation industries.

Given the complexity as well as the loss potential of the exposure, providing cyber Contingent Business Interruption coverage is unlikely to be offered as a standard offering on the market. As there is limited expertise and capacity available in this space currently, this is offered by a few insurers very selectively.

System/ Technical failure: This provides coverage for business interruption caused by Unintentional / Unplanned outage of computer systems. Unexpected technical failure of the Company's Computer System which causes a loss, destruction or modification of Data or Computer Programmes is covered. Technical failure includes failures in power supply, but only if the power supply is under direct operational control of the Insured; over and undervoltage and electrostatic build-up and static electricity.

Carve-back for Bodily Injury and Property Damage (BIPD) exclusion: Cyber insurance policies exclude any actual or alleged bodily injury, sickness, disease or death of any person and any damage to or destruction of any tangible property, including loss of use thereof. With absolute cyber exclusions under other policies becoming increasingly common, there is a need to cover cyber incident triggered bodily injury and property losses, so that they do not fall in a no man's land.

Value Added services

It may be noted that insurers may not offer all services, mentioned below, free of cost and some of them may attract a fee – separately or built in as a part of premium.

Vulnerability scan: Services are provided to remotely scan a business's internet-facing infrastructure to identify vulnerabilities that are open to potential exploitation by cyber criminals. The scanning service helps detect and prioritises hidden risks and provides a detailed view of a company's vulnerability status so they can better track, understand, and works towards fixing them.

Proactive shunning and training: Before initiating an attack, criminals often conduct reconnaissance to confirm an IP address is a viable target. Shunning prevents these communications from reaching a network, reducing the risk of an attack. If a network is already compromised, shunning can also prevent communication back to the criminal's

servers, effectively disarming malware. Web-based training is also made available to proactively reduce the single largest cybersecurity risk to an organisation: human error.

Cyber-security information portal: This Portal provides online access to a centralized hub of educational and technical cybersecurity information that can help assist in the prevention of a breach. Resources include training tips, cyber news and articles, cyber risk assessments and a variety of valuable tools and calculator.

Simulation Exercises: How the insured would respond, should a cyber-attack take place? These exercises help test efficacy of the incident response in the event of a cyber-attack.

Chapter - 5
Recommendation of the scope of the cyber liability insurance covers for the present context and for the medium term

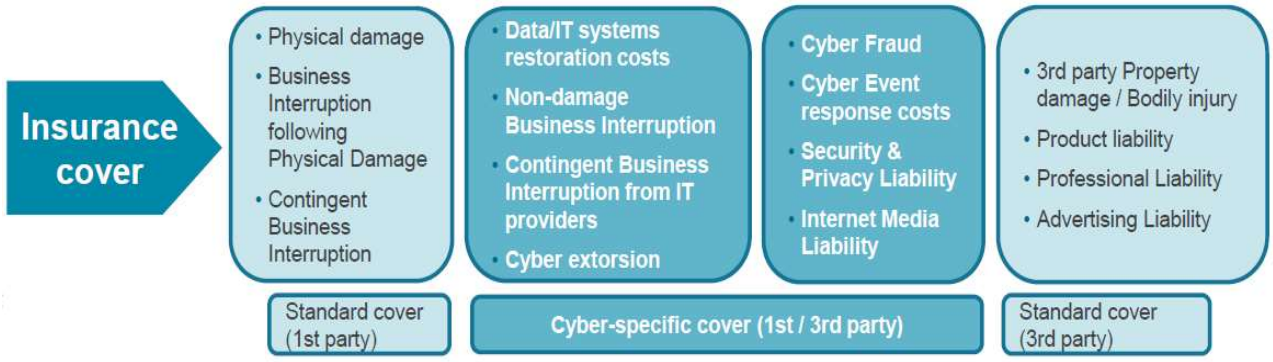
Introduction:

The changes in the cyber risk landscape entails continuous study of the cyber insurance covers to ensure that they respond adequately. While Cyber insurance offerings in India compare well, on many parameters, with that are available globally, enhancement of scope of coverage is always work in progress. As the Indian industry gathers more experience, it can move further to offer covers or services not offered currently.

Any risk to an individual or an organization, accidental or malicious, arising from a loss, failure, or misuse of its own or a third party's information technology systems - this may lead to physical and non-physical losses.

- Physical Loss: e.g.: Property damage, Bodily Injury
- Non-physical Loss: e.g.: Loss of data, non-damage business interruption, extortion, fraud.

These losses are mitigated by Cyber specific and Standard first and third party covers. Further cyber covers are offered as a part of bundled policies or as Cyber extensions within other classes.



- **Standalone Cyber products:** Coverage for losses due to cyber incidents can be categorized by differentiating between losses borne as a direct result of the incident (First party coverage), and losses incurred as a result of litigation by alleged injured parties (Third party coverage). It also provides coverage for other services.

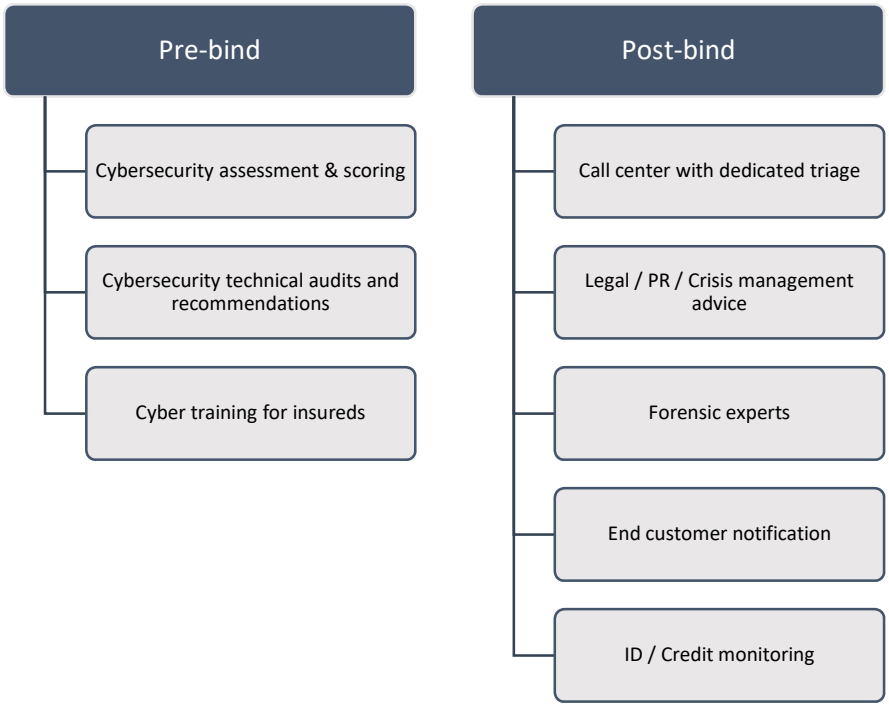
- **Bundled Products:** Cyber covers combined with other lines such as Errors & Omissions Insurance (E&O) and Crime Insurance.
- **Cyber Extensions:** built-in extensions, endorsements, and exclusions carved-back in standard products.

Evolution of Cyber in medium term

There is significant uncertainty in the market on covers to be bought, appropriate limit purchase, and taking right deductible. Attacks on establishments are increasing and every year new cyber incidents are carried out on specific targeted industries. During NotPetya and WannaCry, healthcare, logistics, and manufacturing establishments were targeted, during Covid-19 pharma companies and schools were targeted. Coverages are evolving, more and more demands would evolve in medium term based on new discoveries about these incidents. All these demand that cyber insurance underwriting teams invest more in cyber knowledge to build expertise to properly develop and manage their portfolio.

It is worth noting that cyber insurance is only a part of the service that insurance companies provide. Many other services are also offered during the life cycle of the policy which help the insured in better understanding of the risk leading to prevention and mitigation of losses. These are necessary for both small and large clients, even though the scale varies, as a part of complete solution. Indicative examples are given below. Some of the services may be free and others invite some fee.

Examples of Cyber insurance panel of services



Recommendations for enhancement of scope of the cover for the present context and in the medium term

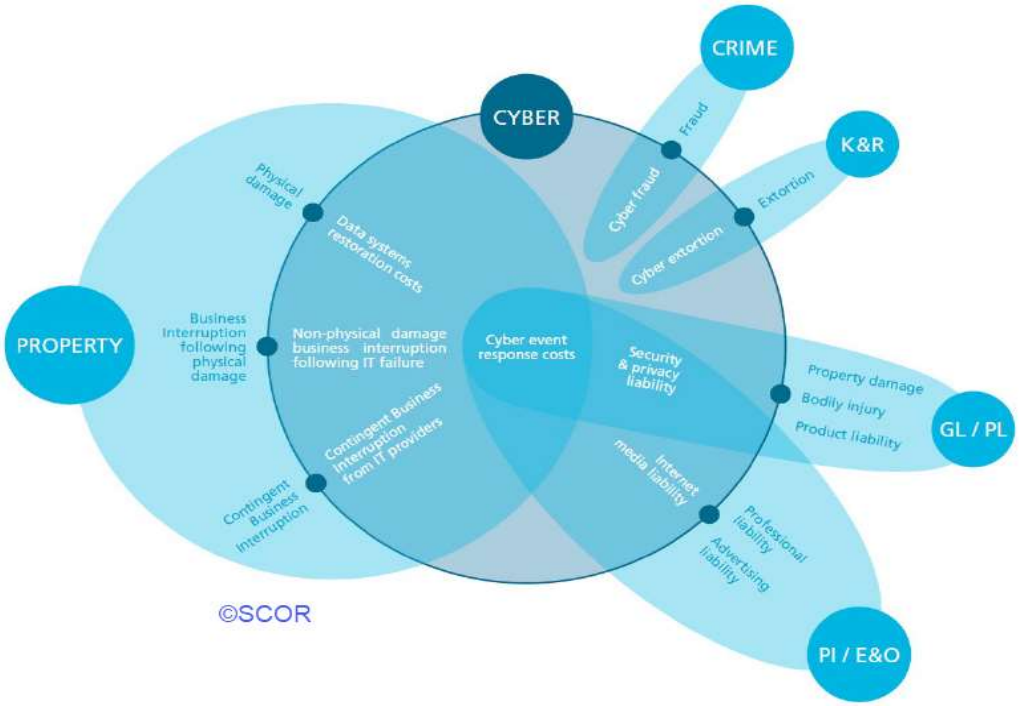
Cyber risks are not static. Therefore, cyber insurance covers cannot be static. It is necessary that as the market evolves in response to the emerging needs, the scope of the cyber policy needs to be enhanced. The Working Group is cognizant of the fact that, cyber insurance being much reinsurance dependent at present, the breadth of the coverage enhancement, the pace of addition and pricing depend upon the perception of reinsurers/insurers about the claims experience and exposures including accumulation exposures in this space in India and globally. Yet, evolutionary hiccups should not deter the insurance industry in keeping pace with technology and the challenges it unfolds.

With this background, the Working Group recommends the following steps and covers to facilitate the development of a resilient and robust cyber space, both in the short and medium term.

Present Context:

- **Addressing Silent Cyber:**
  Insurers may place this matter high on the agenda and address this problem sooner than later. In simple words, it is when the policy explicitly does not exclude or include

coverage. This is also known as “unintended” or “non-affirmative” cyber coverage. Cyber exposure is a concern for all underwriters. Cyber affirmative and silent covers are scattered in many different products beyond Standalone ones. Cyber risk permeates all classes of insurance without boundaries of industries. A cyber event can trigger losses across various lines of insurance – property damage and business interruption resulting from computer systems failure / virus under property insurance, siphoning money through phishing under crime insurance, product liability / recalls from security vulnerabilities under product liability / recall insurance, breach of contract / negligence claims under E&O insurance and for managerial negligence under D&O insurance (FedEx case).



Insurance cover may respond in one of following 2 ways:

- **Affirmative cover:**
  Covered through cyber specific policies for the coverage as mentioned above.

- **Non-affirmative cover:**
  Policy explicitly does not exclude or include coverage. This is also known as “unintended” or “non-affirmative” cyber coverage.

When cyber insurance was introduced in the 1990s, the focus was on covering data breach exposures in response to regulations framed by authorities in USA and Europe. Later, with business operations getting more digital and owing to spread of all-pervasive influence of information technology, insurers started offering wider coverage. But there

was not much foresight about the seepage of silent coverage in other lines of insurance like property, marine and general liability insurance etc. Many property and liability insurance policies were designed when cyber wasn't perceived as a major risk. These policies often did not explicitly mention cyber coverage. While the insurance fraternity debated this issue as a part of regular review of operations, albeit at a low volume, the devastating NotPetya attack and other high-profile cyber security events, in the recent past, have placed the issue high on the agenda for the insurance industry.

Having recognized the need to avoid assumption of unintended exposures / losses Insurance Regulators have also expressed concerns about lack of certainty in Policy coverage and inadequate risk assessment, in response market has engaged a clarification process.

- PRA (Prudential Regulation Authority, UK) was first to express concerns in 2019: "All insurers should have action plans to reduce the unintended exposure which can be caused by non-affirmative cyber cover"

- Lloyd's responded in a staged approach addressing all (re)insurance classes in 4 phases (January 2020 July 2021) and LMA (Lloyd's Market Association) panels subsequently issued Cyber clarification clauses: "Lloyd's underwriters are required to ensure that all policies affirm or exclude cyber cover".

- Most large insurers have also issued Cyber endorsements to their P&C products.

It is necessary to address this issue and ensure that all policies either affirm or exclude cyber cover leaving no scope for vagaries of future interpretations. Listed below are some of the common exclusions in the market which take away the cover

- Insurance: NMA 2914; NMA 2915; CL380; NMA 2981; NMA2982 …
- Reinsurance: NMA 2912; NMA 2928; IT clarification agreement …

NMA 2914, NMA 2915 excludes non-physical loss only,
CL 380: excludes physical and non-physical loss

- Most of these clauses have been drafted in the early 2000's and are not capturing the most recent developments of Cyber risks
- As an attempt to clear these issues, new clauses are being drafted for various markets: property (LMA, IUA), engineering (IMIA), aviation (AICG), etc.

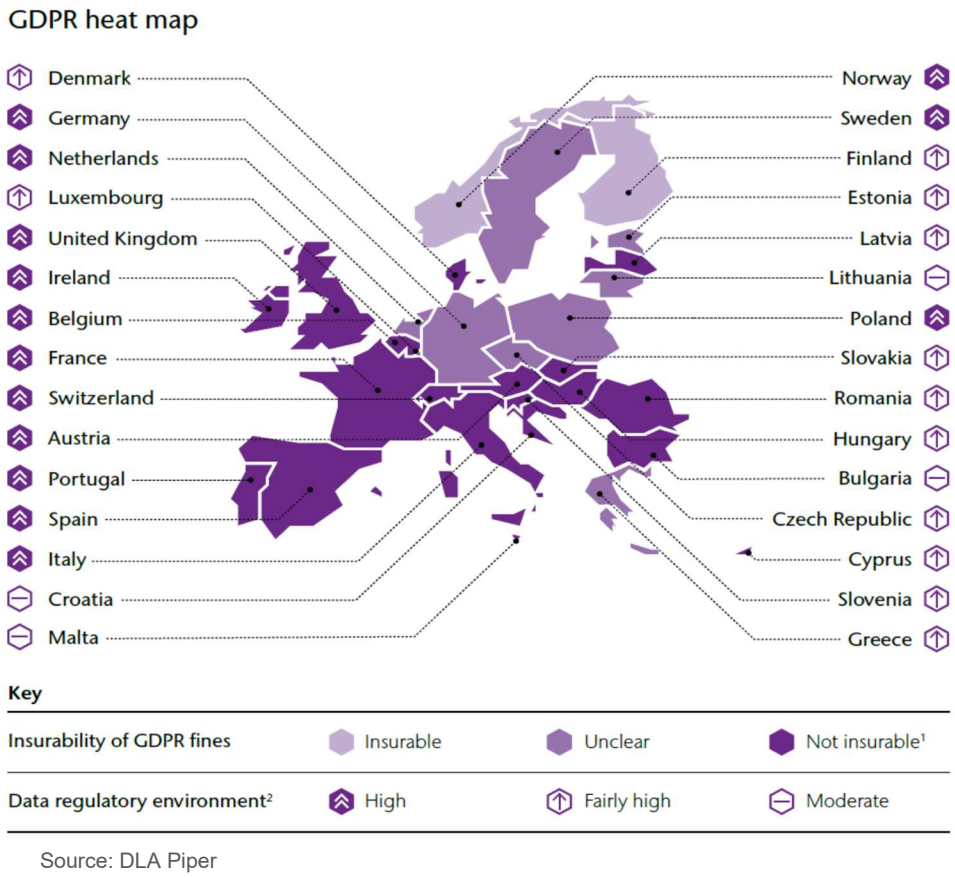
IRDAI may consider issuing guidelines to all insurers to address this silent cyber issue within a specified timeline. The need is pronounced for all risk policies like IAR/ CAR/EAR etc. where basic coverage is governed by the erstwhile tariff. The transition to affirmative coverage for cyber risk needs close monitoring to ensure that major gaps in coverage do not emerge based upon the application of exclusions of cyber risk.

- **Comprehensive Solutions:**

Insurers must work towards offering comprehensive solutions rather than mere loss mitigation products, not only as a customer friendly initiative but also as a good risk mitigation measure. The bouquet of services has been discussed earlier in the chapter.

- **Clarity relating to some payments:**

Insurers should strive to bring clarity to coverage on fines and penalties which remains unclear at this moment as discussed below. It is now well known that GDPR has exacerbated exposure to regulatory fines and question of insurability. It is found that in many EU countries, such fines are not seen as insurable since contrary to public policy.



Source: DLA Piper

- **Bricking costs:**

Cyber products usually cover costs to replace / restore / recreate data and software that have been destroyed, corrupted or damaged and not the Computer System itself (computer, server, mobile phones, Industrial control systems, etc.) using / storing such data or software. Purpose of this extension is to cover replacement costs for such equipment that is rendered useless for its intended purpose.

- **Removal of Reference to Targeted intrusion:**

Targeted intrusion refers to intrusion by the attackers to identify a target and then infiltrate the target's network to achieve their objectives. Some of the policies currently cover only targeted intrusion into the computer system which is mostly not the case. The attack is usually targeted to multiple web users/content users and the said condition again leaves a gap in the coverage. Given the need for this cover, insurers may remove reference to targeted intrusion and extend cover as long as it is unauthorised.

- **Bodily injury and Property Damage (BIPD):**

Cyber insurance policies exclude any actual or alleged bodily injury, sickness, disease or death of any person howsoever caused Property Damage and any damage to or destruction of any tangible property, including loss of use thereof. With absolute cyber exclusions under other policies becoming increasingly common, there is a need to cover cyber incident triggered bodily injury and property losses, so that they do not fall in a no man's land.

- **Contingent Business Interruption:**

It covers business interruption loss and expenses incurred as a result of an interruption, degradation of service or unplanned suspension of a supplier / receiver Computer System. It creates exposure to third party IT systems which are commonly used as entry point for cyber-attacks. The cyber contingent business interruption risk of an insured single company is characterised by the exposure and the information security level of the relevant provider of IT services or of the suppliers of goods. There are insured organisations which represent a higher exposure than others by virtue of their industry sector. For example, there is an above average dependence on IT services by retailers, financial institutions, and IT service providers themselves, as well as by organisations active in the tourism, hospitality, logistics and transportation industries.

Given the complexity as well as the loss potential of the exposures, Cyber Contingent Business Interruption coverage is being provided on a very limited scale currently

Medium Term:

- **Cyber Reputation loss:**

Covers loss of net profit that a company is prevented from earning due to damage to company's reputation caused by a Cyber-attack. Most of the policies currently offer coverage for mitigation and crisis management expenses to preserve reputation / image of the insured. The widened extension can also cover business interruption loss as a direct consequence of a reputational damage. In this context, it may be noted that lack of clear measurement of impact of reputation damage on income makes loss assessment/ adjustment challenging.

- **Coverage for Hardware Betterment costs:**

These include digital asset replacement costs the insured incurs due to the alteration, modification, deletion, denial of access to, damage, corruption or destruction of digital assets. Hardware betterment expenses include increased memory capacity or processing speed necessary to install more secured IT system standard technological advances. These may be necessary to prevent the re-occurrence of alteration, modification, deletion, denial of access to, damage, corruption or destruction of digital assets caused by a security event.

- **Voluntary shutdown**:

Following a cyber-attack, particularly manufacturing companies may have to temporarily shut down/ isolate some of their facilities when they are on the same network to take required preventive actions after the detection of the cyber-attack. This in fact may help avoid spread of the loss.

Chapter - 6
Exploring possibility of developing standard coverages, exclusions, and optional extensions for various categories

Before exploring the possibility of standardisation of coverage, it is necessary to examine various aspects relating to cyber insurance in India including coverage issues, sector wise exposures, underwriting and pricing methodology, claims response and management.

The Working Group have reviewed and reflected on the existing coverage, exclusions, extensions, underwriting practices and claims processes prevalent in the market and also looked at industry specific risks, trends and implications. Cyber liability insurance in India is still evolving and the current ecosystem allows it to innovate and bring solutions to the market with agility. As the cyber insurance market evolves, some amount of convergence would emerge among players on best practices and this section of the report will help provide a point of reference to underwriting, claims, reinsurance, services, sales and other practitioners operating across the cyber insurance segment in India. Coverage aspects, extensions and exclusions have been extensively discussed in chapter 4. Other relevant matters are as under.

Underwriting and Pricing Methodology

Cyber Risk Insurance is different from other Insurance coverage as there is no standard scoring systems or actuarial tables for rate making. Cyber risk is a relatively new concept, and data on security breaches and losses either do not exist or exist only in miniscule quantity. The issue is further exacerbated by the reluctance of organizations to disclose details of their security breaches as it could lead to loss of market share, loss of reputation and so forth.

Modelling Cyber risk is inherently extremely challenging due to

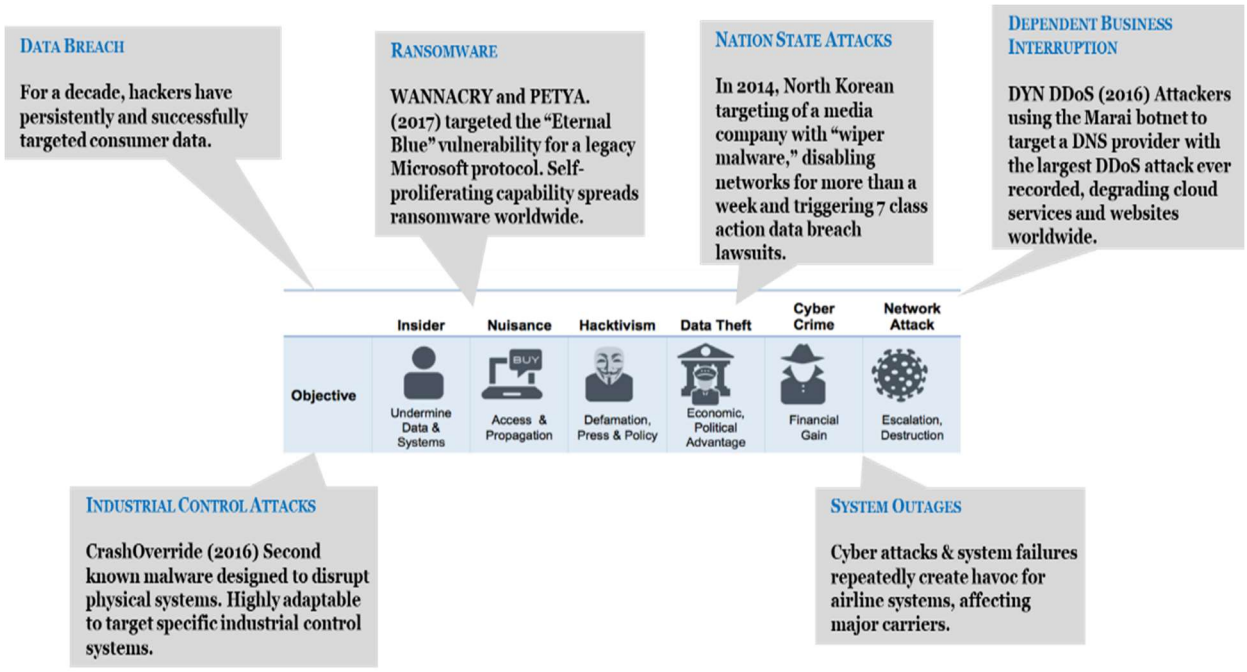
- lack of available and standardized cyber incident data, and
- the continuously and rapidly changing nature of risks.

Available data on cyber risk underwriting is at a very nascent stage because of which standardized and established strategy for pricing and assessment is still far-fetched as the actuaries do not have the data sets of the standard that they are used to working with.

The need of the hour is that all the Insurers capture the data in similar to facilitate more efficient data transfer between the industry participants (client to broker to insurer to

reinsurer) which will facilitate anonymous data sharing mechanism for the benefit of the entire market.

As per Institute and Faculty of Actuaries, Cyber is an Evolving risk. There are many factors are many factors involved which in turn result into many attacks as highlighted in the Figure below with examples.



(Institute of Faculty of Actuaries – Cyber Pricing)

Meanwhile, insurers rely on certain common underwriting practices to evaluate cyber exposures for each insured on a case specific basis.

1) Scale, Scope and Type of Insured's operations
   a. Turnover, Employee strength, geographical spread
   b. Type of services/business/products offered – Industry specific cyber threat vectors
   c. Level of Outsourcing and partners involved

2) Nature of data held by the insured and the security framework around it
   a. Data protection and Privacy policy followed by the Insured
   b. Compliance with ISO, GPPR and other data protection guidelines laid across geographies
   c. Data access (firewalls, access restrictions, etc.) and recovery plans (data back-up and recovery framework) – IT and Network security plans

3) Understand the technology framework of the insured including the level of inter-connected ness and related vulnerabilities
   a. Operations Technology layout and framework (extent of Inter-connectedness)
   b. Operations Technology data back-up and recovery plans

4) Crisis management and Resilience plans – Business Continuity plan, Crisis Management plan

5) Past Cyber incidents – Type and extent of loss incurred, and remedial measures undertaken

Insurers could also undertake further assessment measures like:

- Cyber scanning tools and reports that offer a view of potential cyber vulnerabilities of the Insured and cyber risk grading
- Detailed security risk assessment through in-house or third-party cyber security agencies
- Tabletop discussion with the Insured to get an in-depth view from the Insured

Claims Response and Management

The liability linked to cyber exposure can have devastating effect on the businesses. As much as it is important to have robust systems in place to avoid cyber incident, it is all the more important to have effective system in place to respond and manage the situation when a cyber-incident occurs.

As companies rely more heavily on their IT systems, the business interruption associated disruption becomes even more substantial and detrimental. At the same time, ransom-ware attacks are increasing in sophistication and are even infiltrating backup systems.

The costs and expenses associated with a cyber-incident can be categorized into four segments.

Assistance and Emergency Measures	Restoration Costs and Additional Expenses	Liability Coverage	Loss of Turnover and Increase in costs
▪ Identification, assessment, and containment of security event (IT forensics).	▪ Restoring the IT system to its state prior to the claim. ▪ Maintaining operability of the IT system. ▪ Preparing the claim.	▪ Defence costs and damages arising out of claims made by third parties: ▪ A security event.	▪ Business interruption. ▪ Extra expenses.

▪ Provision of legal assistance (data breach of confidentiality). ▪ Provision of crisis management or communication assistance.	▪ Preventing or mitigating a liability exposure/detecting and controlling any improper use of personal data (data breach). ▪ Communication strategy. ▪ Notification to the authority or to individuals (data breach). ▪ Ransom. ▪ Defence costs resulting from an investigation by a regulator. ▪ Regulatory fines by national authorities for data protection rights violations, such as the GDPR.	▪ A breach of confidentiality of personal data. ▪ Defamation, damage to reputation, breach of intellectual property, violation of privacy, etc.	

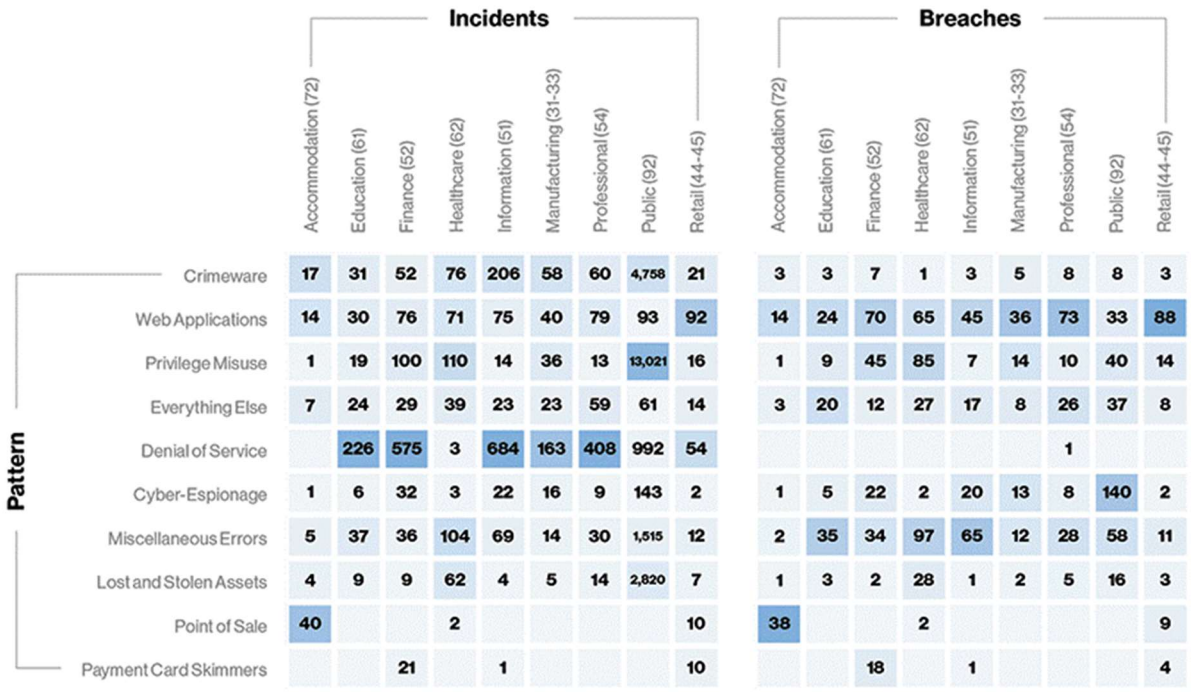
Considering the complex nature of cyber claims, it is common for Insurers and Insureds to appoint Claims/Incident Response Consultants who could offer Incident response, legal and IT forensic services for the Insured. Such consultants could also assist in ransom-ware claim management.

Industry Wise Cyber Exposures

The advancements in technology and its usage have connected people, businesses and organisations in India and brought them closer, leading to economic progress. However, these advancements come with critical vulnerabilities which can be exploited by those who are experts in misusing technology for economic gains. As corporate systems get more interconnected, another significant factor the industry is grappling with is the increasing number of breaches and sophisticated cyberattacks.

India was ranked among the top five countries to be affected by cybercrime, according to a 22 October report by online security firm “Symantec Corp”. In September 2020, the Ministry of Electronics, and Information Technology (MeITY) told the Parliament that Indian citizens, commercial and legal entities faced almost 7 lakh cyber-attacks till August this year. A PwC study estimates that the cyber security market in India will be defined by three key sectors—banking and financial services industry (BFSI), information technology (IT) and information technology enabled services (ITeS), and government. These sectors will constitute 68% of the cyber market share.

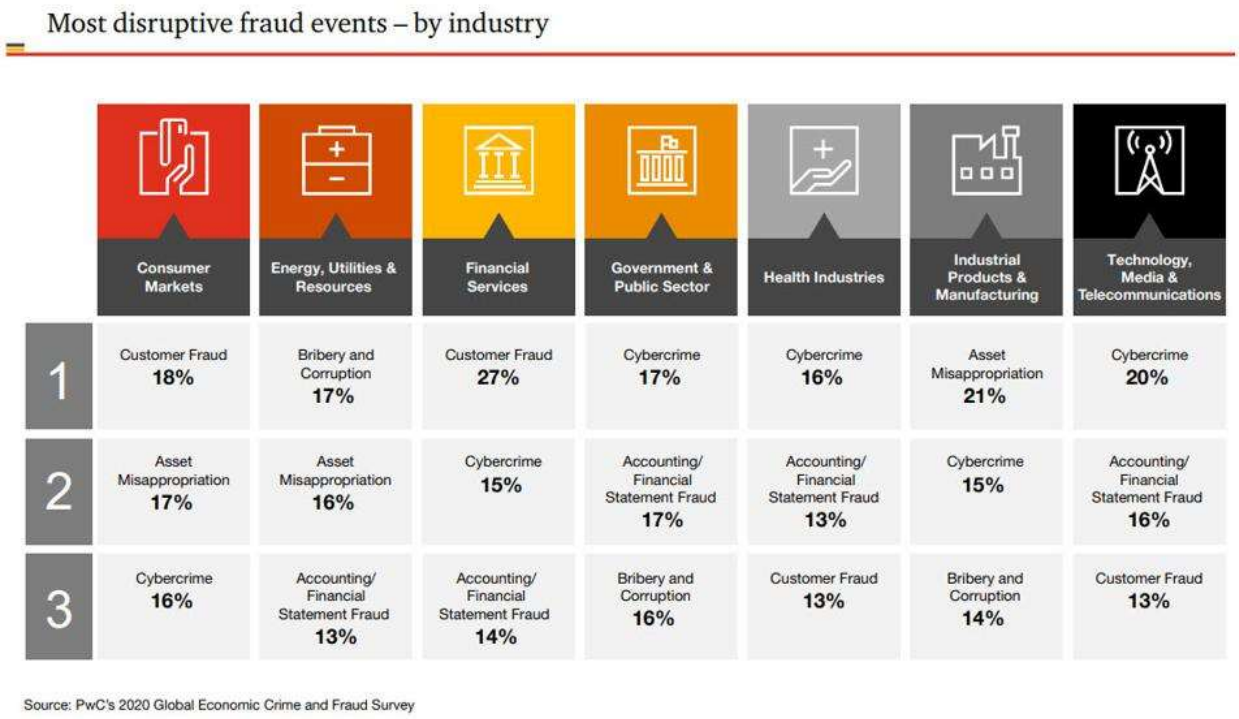
Reports published by several leading analysts and consulting firms clearly indicate that while all sectors are observing significantly increased cyber risk; banking and finance, public/government, professional services, information and technology and related industries and healthcare and pharma clearly stand out in terms of incidents.



Pattern	Incidents									Breaches								
	Accommodation (72)	Education (61)	Finance (52)	Healthcare (62)	Information (51)	Manufacturing (31-33)	Professional (54)	Public (92)	Retail (44-45)	Accommodation (72)	Education (61)	Finance (52)	Healthcare (62)	Information (51)	Manufacturing (31-33)	Professional (54)	Public (92)	Retail (44-45)
Crimeware	17	31	52	76	206	58	60	4,758	21	3	3	7	1	3	5	8	8	3
Web Applications	14	30	76	71	75	40	79	93	92	14	24	70	65	45	36	73	33	88
Privilege Misuse	1	19	100	110	14	36	13	13,021	16	1	9	45	85	7	14	10	40	14
Everything Else	7	24	29	39	23	23	59	61	14	3	20	12	27	17	8	26	37	8
Denial of Service		226	575	3	684	163	408	992	54							1		
Cyber-Espionage	1	6	32	3	22	16	9	143	2	1	5	22	2	20	13	8	140	2
Miscellaneous Errors	5	37	36	104	69	14	30	1,515	12	2	35	34	97	65	12	28	58	11
Lost and Stolen Assets	4	9	9	62	4	5	14	2,820	7	1	3	2	28	1	2	5	16	3
Point of Sale	40			2					10	38			2					9
Payment Card Skimmers			21		1				10			18		1				4

Source: 2019 Verizon Data Breach Investigations Report (DBIR)

This is also evident in business disruption caused due to such incidents or breaches in terms of perceived risk in these industries.



We discuss below a few industries with unique characteristics and exposures to better understand the nature of cyber risk in the market:

a. **Healthcare:**
The rapid digitization of the healthcare industry has led to a huge increase in the number of ransomwares, malware and targeted attacks, which puts confidential patient data like personal details, medical history and financial information at risk. The healthcare systems are emerging as an attractive industry for hackers to target with each stolen medical record. During the past years, cyber-attacks on healthcare services have resulted in the loss of hundred thousand of Personal Identifiable Information (PII) and Personal Health Information (PHI) data and resulted in disruption of critical care services.

Implications of cyber-attacks on healthcare across a wide spectrum are critical PII and PHI data loss of VVIPs and HNIs globally could lead to a significant financial and political control by organized cyber-crime syndicates and states sponsoring them. The populated geographies like India can become a rich source of medical research data by virtue of the sheer size of the sample. Advanced attacks like ransomware can cause major operation disruption by holding critical data and assets to ransom. There is financial and brand reputation loss to the healthcare provider in terms of regulatory fees and mistrust.

Healthcare organizations saw a significant increase in malware or bot attacks, with socially engineered threats and Distributed Denial of Service (DDoS) attacks steadily growing, as well.

b. IT and Telecoms:
Cyber-attacks are increasingly targeting the technology and telecom sector. The complexity of a tech company's risks depends on the type of products and services the company provides. Some companies may be required to store large amounts of sensitive data, while other companies need only maintain smaller amounts of information on their customers. Still, any stored data is a vulnerability, and any security incident can result in negative press, a potential stock devaluation and an overall lack of trust in the company holding or servicing your data.

Telecom and network service providers, Cloud storage providers, Cloud computing services, Developers of cyber security software, or a file-sharing solution provider, are often the targets of cyber-attacks. The damage such attacks can inflict go far beyond the cost of recovering compromised data. As these companies are often a gateway into multiple businesses, the ultimate aim of direct

cyber-attacks is to access the core infrastructure of a telecom or technology company. Companies may suffer huge losses in terms of Third-party clams for privacy breach, Ransom ware, Business interruption, regulatory investigation and fines and penalties. In case of a cyber-incident, they may also need to assess, aid, and resolve any impact to corporate client systems and data exposed.

c. Banking and Financial Services (BFS):

Due to the high value of financial data, cybercriminals are increasingly targeting customer banking credentials when carrying out attacks. An International Monetary Fund (IMF) study suggests that the average annual potential losses from cyber-attacks could be nearly 9% of banks global net income i.e. around $100 billion. And in cases where the attacks were severe, the loss estimate could range from $270 billion to $350 billion. In rarest of the rare cases, the average potential loss could be as high as half of a bank's net income, which could put the entire banking and financial sector in jeopardy.

As more banks implement mobile banking applications, new vulnerabilities for cybercriminals to target are introduced to the network. Banking apps can be exploited from both the client-side or the server-side, making them difficult to secure. This means that banks must be able to ensure that data is secure when it is being accessed from a customer device as well as when it is stored on bank servers. Cybercriminals also attempt to target bank's third-party vendors (software vendors, banking equipment vendors, customer service vendors). Vendors have access to critical banking data but often lack stringent security policies, making them a prime target for threat actors.

According to Cyber Risk Services at Deloitte, hackers from various countries attempted over 40,000 cyber-attacks on India's Information Technology infrastructure and banking sector over five days in the last week of June 2020.
Malware has long been a threat to the banking sector. By infecting vulnerable end-user devices with malware, cybercriminals are able to gain access to entire banking networks and steal critical user data. With malware becoming easier than ever to obtain, this threat has grown in recent years as in 2019, it was responsible for 75% of all data breaches in the banking sector. In addition to malware attacks, phishing attacks i.e. communications, such as emails, calls, or texts, that impersonate company officials in order to trick customers or employees into sharing information is another common risk.

d. **Manufacturing:**

Given its focus on innovation and an increasing reliance on connected products, the manufacturing industry is also vulnerable to cyber risks. As the manufacturing industry is undergoing industrialization by leveraging IoT, digitization, cloud computing services for their productivity enhancement, resource management, and creating cost efficiencies is more vulnerable to cyber-attacks. According to Quick Heal, a cybersecurity firm the Indian manufacturing sector faced 27.56% of total cybersecurity attacks in the 1st quarter of 2019.

Given the highly connected environments manufacturers work in, and the pace of technological change they face, cyber risk is a top-of-mind industry issue. In fact, nearly half of the executives surveyed by consulting firm Deloitte lacked the confidence that they are protected from external threats, and it is increasingly important for organizations to assess their organization's risk profile and preparedness in the event of a breach or cyberattack.

Apart from the loss of revenues/market credibility and the operational disruption caused by successful cyber-attacks, they will also now be hit with heavy financial penalties imposed by regulatory bodies for every security breach.

Manufacturers with inadequate cybersecurity also risk their intellectual properties (IP) such as new technologies/products, confidential designs/formulas, and manufacturing processes being compromised by outside actors and internal threats. These IPs can then be sold to potential buyers, including competitors, or heavily advertised across the Dark Web.

The exposures get compounded for organisations that are listed or are operating in more litigious jurisdictions.

Cyber Solutions for MSME segment

In 2019, 43% of all cyber-attacks worldwide were aimed at SME's. MSMEs in India face the same threat and trend. Hacker's target them because of their less sophisticated IT security infrastructure Data security council of India is committed to promote cyber security awareness among these sectors. Such incidents can result from a wide range of causes, including hackers, malware/virus, malicious insiders, lost or stolen laptops and employee error.

Lack of awareness, complex policy structure and wording, affordability and underwriting requirements are key barriers to increase cyber insurance penetration in this segment.

Shared industry awareness programs, simplification of product constructs and underwriting processes and competitive pricing can aid secure digital adoption for MSMEs in India and help unlock the market potential for insurers.

At the minimum, it is necessary to offer to MSME sector coverages that include first party coverage, third party coverage and coverage for other services as mentioned in Chapter 4. A digital first approach providing self-service solution for MSMEs and insurance intermediaries, automated rules-based underwriting and claims and service model would help the industry serve this segment and improve reach and affordability. Due to low awareness on exposures and required security measures, challenges in this segment cannot be addressed through cyber insurance alone. For any initiatives relating to MSME sector, to begin with it is a good idea for the insurers to take the definition for MSMEs as defined by the Government of India.

Normally, the coverage terms for MSMEs are broadly similar to those offered to other corporate customers. However, considering the vulnerability of the MSMEs who might not be having highly sophisticated control systems to prevent cyber incidents, insurance industry should ensure that coverage terms do not become too stringent and also make efforts to demystify cyber coverage through initiatives such as dissemination of information on coverage provisions, safety standards and by incentivizing adoption of possible safeguards. Coverage for MSMEs should facilitate a quick resumption of business after an incident, by offering all allied recovery services as a bouquet. An ecosystem approach involving insurers, cyber risk consultants and solution providers, insure-tech companies, industry bodies, financial institutions and digital platforms can help accelerate awareness and adoption

While policy wording and coverages are important, it is education and supportive ecosystem which matters most for spread of cyber insurance culture in MSME sector

Standardisation of Cyber Insurance Policies:

Our review of the market suggests that cyber insurance segment is still in nascent stages and being closely linked to rapid evolution of technology. The risk profiling and industry coverage needs are expected to change over the next few years. A few aspects that would impact cyber insurance offering by insurers and reinsurers in the market are:

Ever-evolving cyber threat landscape: Cyber-attacks have an inherent volatility as they keep evolving over time, which limits the value of historical experience and undermines the exposure's predictability. As a result, existing cyber threats keep mutating, while new ones are continually arising. As companies adapt to one type of attack, threat actors keep

coming up with new techniques, targets, and points of entry to exploit. New legislation and regulations are in development and this may lead to requirement of new insurance solutions.

Digital adoption by industries yet to peak: While digital adoption and technology adoption across industries has accelerated in the last few years, several industries & corporates are still investing and evolving. It means that the business and operations models, technology infrastructure and services are yet to hit a point where risks are well understood. For example, Industry 4.0 as a theme in manufacturing is expected to see a huge boost once 5G telecom infrastructure is launched in India which may transform businesses but also significantly shift cyber risk profile.

Lack of historical loss data: Cyber insurance is a relatively new line of insurance and hence there is lack of historical data with insurers, which makes it difficult to build the predictive models that can help assess probability of loss. There is also no comprehensive, centralized source of information about cyber events for insurers to refer. In addition, a large percentage of cyber losses aren't even acknowledged to outsiders especially cyber events such as denial of service attacks, ransomware, and theft of intellectual property are often kept under wraps.

In view of the foregoing, insurers need to frequently adapt and change their policy wordings, question sets, and underwriting approaches in order to ensure that they are best serving their customers while managing their exposures prudently. Insures also need to adapt based on risk evolution in domestic as well as international markets and reinsurance policies & capacities available.

Cyber insurance, being a new product, is supported by international reinsurers for the innovation, technical knowledge, product wording and various other services. Instead of a standardized wording they may prefer to use coverage and exclusions as per the latest developments in the market

The Working Group believes that, while standardisation is a very good approach, early standardisation of cyber insurance in its nascence may impede innovation and adaptation to evolving industry needs. It may lead to price-based competition instead of being agile and contextual to client needs. Nonetheless, there are certain aspects of cyber insurance that require a consensus and Common Reference Framework to bring about clarity in coverage. The recommendations of the Group on some of the issues that need to be addressed are listed below:

a. **Computer System:** Some policies contain a provision that coverage is provided to those systems which are provided by the company for exclusive and secure usage for

the purpose of its business. This may deny coverage when employees use their own computers while working from home which is more prevalent now, in the post Covid19 world. Given the compulsion for and encouragement given to employees to work from home, it is necessary to include their own devices too. So also, other devices, tablets, mobile phones etc. which are used for official purposes, albeit with required safeguards. It is necessary to provide coverage for all these aspects explicitly

b. **Regulatory fines and penalties Coverage:** Cyber insurance policies provide cover for fines and penalties "*to the extent insurable by law*" i.e. the law applicable to the policy and the jurisdiction in which the payment is to be made. Ambiguity in this matter arises because the issue of insurability is normally not directly addressed in the statute or in the regulatory provisions, the one known exception being the UK Financial Conduct Authority's prohibition of insurance payments to reimburse the cost of financial penalties it imposes. Further, there are jurisdiction related issues – some favorable to allowing such coverage and others and others not. One way to address this issue is to identify the kind of fines payable and confirm coverage under favorable jurisdiction.

c. **Intentional Acts exclusion:** Cyber policies exclude coverage for Dishonest or Improper Conduct of employees, however this could be modified to make it applicable only for Key personnel of a company i.e. Chief Executive Officer, Chief Financial Officer, Chief Risk Officer, General Counsel, Head of IT department, Head of HR department, Data Protection Officer and Chief Compliance Officer or any other Person in a functionally equivalent position.

   Further, insurers can advance Defence Costs until there is
   i. a final decision of a court, arbitration panel or Regulator, or
   ii. a written admission

d. **Bodily Injury and Property Damage Exclusion**: Cyber policies exclude coverage for claims arising out of "bodily injury" and "property damage" as these would find coverage under casualty, property, and marine policies. However, coverage for claims alleging mental anguish, mental injury, shock, emotional distress, and humiliation are carved back, as claimants may cite these injuries as damages stemming from a cyber incident. With absolute cyber exclusions under other policies becoming common, there is an urgent need to consider covering cyber incident triggered bodily injury and property losses, so that they do not fall in no man's land

e. **War, Terrorism, Invasion, or Insurrection Exclusion:** All cyber policies exclude coverage for loss from acts of war, terrorism, invasion, and/or insurrection. The exclusions are often written expansively and given the proliferation of state-sponsored,

political, and ideological cyber-attacks, could exclude coverage for most security breaches. However, insurers could modify these exclusions to carve out coverage for "cyberterrorism" or "electronic terrorism"

f. **Failure to maintain minimum security standards:** Some cyber policies exclude coverage for claims based upon the insured's failure to maintain minimum security standards. While the wording varies from insurer to insurer, and at times they are placed as recommendatory measures, this exclusion may deny coverage, sometimes in unexpected ways. If this exclusion is tied to the standards mentioned in the proposal from, policyholders need to be careful to accurately complete cyber insurance proposal form and ensure compliance with the security standards mentioned therein are maintained throughout the policy period. But, to avoid the risk of any wrong application of this exclusion, it is desirable to consider specifying that this exclusion applies only when the failure is material to a cyber loss.

g. **Changes in the risk:** If material changes in the risk are not informed to insurers, policy rights may get prejudiced. There may be changes in the fund transfer protocol, changes in the business continuity planning and access control for remote access. It is necessary to seek continuity of coverage by informing insurers about the changes lest coverage gets impacted adversely. Need for this notification to insurers has become more pronounced after Covid 19 lockdown when work from home has become a norm and other processes also had to undergo significant change. While the insurers concern to ensure that the risk underwritten and the risk subsisting at the time of loss are the same is understandable, the notification of risk changes should not be so onerous as to deprive the insured of a claim even when such changes are not material to the loss.

Chapter - 7
Other Matters of Relevance

1. Remote Working: The New Normal:

Even before the pandemic, there was a slow, but gradual shift of the workspace from the office to home. The pandemic has propelled this shift to a new reality, which could continue to be a permanent feature of the future of work. With many employees around the globe working remotely, steps need to be taken for bolstering IT security in the home office: Some of the suggested measures are:

- keeping software up to date
- activating virus protection and firewalls
- being increasingly cautious about sharing personal data
- Making sure web browsers are up to date
- keeping passwords safe and changing them regularly
- protecting confidential emails with encryption
- Only downloading data from trusted sources
- making regular backups
- turning off voice-activated smart devices and covering webcams when not in use
- making clear distinctions between devices and information for business and personal use and not transferring work between the two
- identifying all participants in online sessions
- Logging out when devices are no longer in use and keeping them secure
- following security practices for printing and handling confidential documents
- being careful with suspicious e-mails or attachments

2. Accumulation Issues:

Cyber loss exposures emanate in many ways -

i. Economic loss: Damage to systems/property; Notification costs; Remediation costs to investigate & remedy breach

ii. Liability exposures: Damages by customers, vendors, business partners triggered by errors & omissions or failure to protect data

For primary insurance companies the risk accumulation within their portfolio of Cyber Policies may expose them to accumulation risk and higher financial losses. A single event generating a widespread impact on thousands of businesses at once is another distinct possibility. For example, a single malware attack could breach multiple client

network at one point. The major cyber accumulation risk scenarios are essentially man-made and in addition to the malware attacks and attempted data breaches, technical failures can also have devastating consequences. Hence, it is essential for an insurance company to actively identify, quantify, model, manage and control cyber accumulation risk.

Accumulation Scenarios:

Ransomware and malware attacks in the recent past have affected businesses causing huge economic losses. These attacks proved to be globally contagious, infecting organizations across multiple countries & geographies.

It is evident that in cyber a significant accumulation potential on a global scale arises from shared software or hardware vulnerabilities, the disruption/outage of central IT services, and attacks on critical infrastructure, such as power supply or telecommunications networks – including the internet. Each of these events may cause various types of financial losses to thousands of companies, and hence poses a major accumulation loss potential.

Challenges in accumulation control:

Tracking the accumulation exposure in traditional property class of business has matured with modelling tools available for measuring earthquake and flood exposures. With cyber risks, the contours of systemic accumulation are not as clear. Accumulation in Cyber Insurance is also a function of the Cyber Insurance coverages provided. Cyber risk is clearly systemic – it is spread through interconnectivity: the internet, communications, and internal and external networks. These connections are neither obvious nor easily tracked. Following are the main challenges faced –

- Identifying dependencies among the risks, defining the different scenarios, and assessing severity of a single event affecting many risks that are affected
- The frequency and severity of cyber events as well as their interdependence are not easy to establish, making it difficult to assess potential aggregation of losses as new and unforeseen attack patterns emerge constantly
- Lack of awareness of potential cyber losses
- Hidden cyber exposure within existing coverages

Quantification approaches for cyber accumulation risk: As cyber insurance in India is still in a nascent stage, the common approach of quantification of accumulation is the

aggregation of full policy limits in the portfolio. This is a very conservative and restrictive approach. In developed cyber insurance markets, insurers are relying on deterministic scenario analyses to quantify the risk. Realistic Disaster Scenario (RDS) modeling for bottom-up measurement of exposure on an event basis is becoming part of cyber framework. The probabilistic modelling of scenario events is considered ideal to assess potential cyber losses, but their development is in early stages.

To address this problem, insurers should closely work with reinsurance companies and modelling firms to develop a cyber risk framework.

3. Cooperation between various agencies:

Considering the pervasive nature of cyber risks, it is desirable that there be cooperation between insurance industry and other technical bodies like CERT-in (part of Ministry of Electronics and Information Technology and a nodal agency to deal with cyber security threats like hacking and phishing also responsible for strengthening security-related defence of the Indian Internet domain) and professional bodies like FICCI (which plays an important role in formulation of economic and finance policies), CII (works to create and sustain an environment conducive to the development of India, partnering industry, Government and civil society, through advisory and consultative processes.) and NASSCOM (trade association of Indian Information Technology (IT) and Business Process Outsourcing (BPO) companies.) etc. This can help understand the changes that are taking place globally with potential impact on Indian market and facilitate exchange of ideas and information on cyber security, economic, finance policies and Insurance. Moreover, this shall provide a consolidated domain with current trend of industry practices, current trends in terms of hacks including proactive steps for loss prevention, impactful solutions developed by various companies and challenges faced in executing the same. This would also provide a common platform to harmonise current industry practices, to glean current trends and to promote proactive measures for loss prevention. Insures can consider sharing amongst themselves information on incidents without breaching confidentiality norms.

4. Cyber Literacy and Education Index:

India occupies 45th position in this index which measure the population's cybersecurity knowledge as well as the ways that countries can enhance that knowledge through education and training. It may be a good idea for the insurance industry to work with concerned authorities and organisations to promote cyber literacy.

5. Developing an enabling cyber insurance ecosystem:

Given the complexities surrounding the technology space, cyber insurance is expected to not only act as a loss mitigation mechanism, but also as a risk mitigation device. Expertise needs to be developed on the morphing challenges technology presents and the threats confronting technology deployment. These include developing a risk evaluation framework, promoting risk improvement measures, incentivizing establishment of safeguards, immediately responding to incidents, recovery, forensic audit and a host of other services that require considerable expertise and knowledge. The insurance industry should collaborate within itself, and with other stakeholders in developing a robust ecosystem of experts and professionals who are equipped to confront the formidable disruptions the threat actors heap on society and to provide mitigation. Insurance industry should act as a facilitator for the growth and development of technology without disruptions. To this end, the industry should identify and benchmark reliable service providers to address each area of specialized response. Insurance industry should also promote sound loss assessment standards and practices.

Summary of views from various stakeholders

The Working Group, during its meetings on online platform of WebEx had interacted with representatives from various stakeholders and also collected responses for extensive deliberations on the subject. The inputs offered by them are summarised as under.

Insurers/ Reinsurers:

The general feeling is that awareness on cyber exposures as also about cyber insurance is low, in spite of a marked increase in cyber incidents. Need for education and creation of awareness is emphasized by all.

On individual Policies:

Individuals perceive payment and back account hacks to be a bigger problem, while companies are worried more about data breach and network interruption.

Coverages offered by most of the Insurers in respect of individual insurance are majorly similar in nature, with the exception of some enhanced covers offered by a few. Theft of funds is seen as a major exposure for individual cyber insurance policies. Some people have an impression that because of the Zero liability concept for the customers of a bank, even this exposure is considered to be close to NIL. While standardisation is a good idea, since there are challenges in its formulation and implementation, it is good to list minimum covers in an individual policy.

There is a need for simple and easy to understand policy wording. One important aspect in the individual policies is that the settlement of claims should be very prompt. Otherwise customer could lose interest.

On popularizing individual cyber, group propositions would work better. This helps in in getting volumes and spreading of risk. Web aggregators, Bancassurance, affinity programmes are seen as effective media to popularize this insurance. It is also believed having a bundled cyber policy with other policies like House Holders package policy may work well.

Standalone individual cyber policy does not seem gaining much traction globally. It is gaining ground, when sold as a bundled policy.

Renewal of individual policies is seen as a problem. Forensic costs and ransom claims are contributing more to claims currently.

There is a need to educate customers on Dos and Don'ts relating to cyber security.

On Corporate Policies

Gaps and need for possible improvements in coverage for Corporates: Exclusions relating to Bodily injury and property damage and computer crime are seen as gaps. For manufacturing sector there is a need to add property damage coverage arising from cyber incident. It is also suggested to blend cyber and crime as a solution.

Silent Cyber: Most of the P&C polices have cyber exclusion which remove the silent cyber exposure. Non-affirmative/ silent exposures in other lines of business are managed by specific Policy exclusions for Bodily Injury/ Property Damage/ Terrorism etc.

Cyber policies are not industry specific. Most of the insurers consider cyber Insurance policy is generic and broad enough to cater to various industries.

Comprehensive solutions: Insurers are convinced about the need to offer comprehensive solutions rather than just to market policies. Some insurers have arrangements with cyber risk assessment agencies. These agencies conduct IT risk assessment for insureds. Their report captures the positive features of the insured's systems and highlights areas which need improvement. This service is offered on need and opportunity perception. The need for support to MSME in this area is understood, as they do not have in-house capability to handle the complexity involved in cyber incident. Costs for these services are a matter of concern, as premiums are small.

Post Claim assistance: The most important factor in cyber insurance is the claims handling. As regards current claims handling, most of the insurers have various support systems/ arrangements in place with relevant outside agencies for support in respect of

a. Incident Management
b. Call Centre
c. Loss Assessment
d. Public Relations Consultants
e. Legal
f. 24/7/365 Support

Penetration: Considering the increasing awareness and need for this product, and the growing dependence on online payment industry, it is expected that the penetration for this product to grow by at least 25% to 30% in the next 5 years.

Dos and Don’ts: It is necessary to sensitise all stakeholders in this matter. While there is no such guideline being exclusively issued but a general hygiene is considered essential. All employees of the corporate should be sensitized about cyber risk sensitivity and Dos and Don’ts should be circulated for education and compliance.

Every corporate should have a well-documented Business Continuity Planning (BCP)/ Disaster Recovery Plan(DRP) & IT Security plan which should be periodically reviewed and effectively implemented. It is also essential to get third party audits including Vulnerability Assessment and Penetration Testing (VAPT) conducted to assess the robustness of the systems. Proper information classification and regular employee awareness programs are very important. Insurance should be treated only as a risk transfer mechanism and cannot be a replacement for the need to have robust security systems.

Industry Specific Cyber: Cyber insurance product caters to all the Industries. The risk per Industry may differ but the cyber events and losses suffered by any industry are more or less the same. The quantum of loss or exposure to an attack will differ from one industry to another. While certain endorsements are more relevant to particular industries, overall policy wording remains the same.

Accumulation: It is very difficult to manage accumulation in this line of business as a single malware attack could breach multiple client’s network at one point. Basis understanding of the risks already underwritten during the year, in case concentration of book on a particular industry is noticed, conscious efforts are made to quote stricter terms to tighten the scope of cover or seek facultative reinsurance support. Limiting capacity deployment and tracking common service providers are some of the ways to monitor accumulation.

Capacity Constraints: There are capacity constraints for coverage to financial Institutions as an industry. Some insurers have treaty constraints on the capacity with restricted limits and on the number of policies.

Coverage offered under cyber policies in India compares well with global offerings.

It is not a good idea to standardised the policy wording, as it may hamper flexibility and innovation. One can explore standardisation of some definitions and exclusions. A consultative approach is necessary in this regard. Policy should be comprehensive and responsive.

Insurance Brokers:

Even with huge exposure and frequent cases, individual cyber has not got that visibility in the Indian market compared to other personal lines general insurance product. This is due to lack of awareness among such group along with complex policy terminologies, complicated claim process and lack of understanding on indemnification available from banks/e-wallets firms are major roadblocks impacting the growth of individual cyber product. A Process Simplified approach which includes standardised wordings (easy to understand), well defined claim process (including expert assistance as well as credit monitoring services) and a clear demarcation on coverage benefit available under such product and from indemnification from other sources will surely boost the growth of Individual cyber programs. With regard to individual cyber insurance, they feel that the base product to be standardised, which would have several other and broad wordings, however this should in no way stop innovations, and there can be a choice given to customers to buy additional covers, as well as carve out certain exclusions at a price, to make the covers wider and acceptable in the market.

As regards product Innovation for Corporate buyers, the existing products should be revisited; and customised to absorb the amendments with the changing exposure. Different approaches to coverage provide choice to policyholders and allows for innovation resulting into holistic insurance solution.

For corporate customers, Insurance industry should agree to minimum IT security standards for the Insured to be able to buy Cyber Security Insurance.

Brokers should be allowed a cyber consulting practice which not only sells risk covers, but also can provide risk based solutions from IT standpoint either directly or by having a tie up, and these services to be allowed for a fee separate than the brokerage, as these are fairly expensive services. This will not only increase awareness, but also will reduce the intensity and severity of the claims.

Quick access to all support systems in the claim cycle chain like Forensic experts, consultants and advocates will be helpful. Insurers should be encouraged to provide value added services which facilitate appointment of professionals who not only perform loss assessment and survey services but also advise on mitigation and claim containment services to the Insured.

Law firms:

They shared their views on various legislations concerning cyber security and also referred to some case laws in cyber litigation.

On cyber insurance policies, simple wording cyber-crime insurance policies for small enterprises would be good with coverage also providing for notification, consequences, and penalties under the Personal Data Protection Bill, 2019. Coverage must also provide for first party and third-party expenses. With regard to the coverage for penalties, it is necessary that penalties that are insurable must be covered, otherwise they create huge financial burden for the insurance buyers. It is advisable to get clarity about coverage for fines and penalties.

Consultants:

Cyber insurance policies should be structured with simple language to avoid buyer confusion and avoid claim disputes. Awareness about cyber insurance covers should be created through education efforts, directly and via agents/brokers.

Industry should perform periodic assessments to determine changes in threat landscape and leverage internal and external cybersecurity expertise to gather cyber threat intelligence.

Insurers need to assess aggregation of risks with appropriate tools.

Cyber Police:

Police department received more complaints related to Ransomware attacks and the department advises all the organisations to install strong firewall to avoid such attacks.

Every organisation should have its own Virtual Private Network (VPN) system to avoid ransomware attacks and also updating the software frequently.

When people don't want to visit police station, there is facility to file a complaint on-line in cybercrime portal i.e. www.cybercrime.gov.in.

IDRBT:

Technology has transformed the way banking is conducted – from providing services online to customers, to storing data in the 'cloud' and accessing information from tablets and smartphones.

Insurance coverages under Cyber insurance policies are designed to address many variables within the online realm and can include- the liability of the bank arising from Financial Loss, data protection laws, the management of personal data and the

consequences of losing personal identifying information, Repair of banks' reputation, Notification and monitoring costs and Cyber extortion and network interruption.

As regards Zero liability protection as advised by RBI, issues arise when insured does not ascertain all details or share all details or when actual reason for loss is not communicated. Zero liability concept also has exceptions.

Industry Bodies (CII/ FICCI/ DSCI):

Due to the present covid-19 pandemic situation, very large number of people are exposed to cyber threats. It is observed that most of the cyber-criminals are targeting Individuals, MSMES, and other commercial establishments. CII has been in touch with many agencies to get updates on cyber vulnerabilities and also to bring about changes in the ecosystem. OS vendors are constantly sharing updates. CII task force circulates the best practices is trying to make sure that same should reach the last level of employees in the organisation.

This is the right time to develop best practices and increase awareness about cyber security amongst end users, in order to protect the Individuals, MSMES and large enterprises.

Claims are coming from different sectors like**.** E-commerce platforms, banks, Auto manufacturing, machinery manufacturing and IT companies. CII feels that while there is an acceptance about the need for cyber insurance in large companies, small and medium enterprises are untapped. It may be a good idea to think of some basic covers for MSMEs as there are no specific and standard wordings to cover Individuals and MSME. There is a need to make the policy easy to understand and remove apprehensions about claim settlements particularly in the context of exclusion relating to breach of best practices.

Vendor management is also an important aspect in the cyber risk management cycle. Indian Insurance market requires Incident Response Management Service which is very important to identifying cyber incidents, quantifying the loss and indemnity settlement.

Cyber risk assessment is a critical component in enterprise risk management. Currently, only a few consultants are undertaking this activity. It is necessary for enterprises to understand third party obligations. Mapping all the services of third parties and noticing changes should be a continuous exercise.

There should be clarity about all the services rendered by insurers post security breach and claim notification. Remediation services and support are also important. It was observed that the coverage offered is not sector specific. Many MSMEs are low on knowledge about the cyber exposures as also low on financial resources to implement the

best practices including buying cyber insurance. Large corporates and IT companies have good awareness about cyber exposures and Insurance because these companies have tie-up with international clients and have sound financial system and resources.

It appears that Indian insurance industry does not have much experience about cyber security management for critical infrastructure companies. At present more attention is given to data breaches. The government and regulatory bodies have an important role to play to enable the cyber insurance space in the country.

CERT-In:

CERT-In team has discussed some of the major incidents which happened with large companies. They have explained about various vulnerabilities.

Vulnerabilities are divided into three kinds.

1. People vulnerabilities
2. Process vulnerabilities
3. Product vulnerabilities

CERT-In issues guidelines regularly. They feel all the incidents may not be getting reported. CERT-In does not certify best practices. But consultants approved by them may certify.

This page has been left blank

References

India : Cyber Law Ecosystem - https://www.asianlaws.org/gcld/gcld_india.php

Overview of cyber laws in india - https://taxguru.in/wp-content/uploads/2012/10/cyber-laws-overview.pdf

India: Key Features Of The Personal Data Protection Bill, 2019 https://www.mondaq.com/india/data-protection/904330/key-features-of-the-personal-data-protection-bill-2019

Munich Re: Evolving Cyber Regulations in Asia Pacific | Munich Re – https://www.munichre.com/topics-online/en/digitalisation/cyber/evolving-cyber-regulations-in-asia-pacific.html

GDPR Key Provisions - https://www.dixonwilson.com/technical-updates/gdpr-key-provisions

What are the key provisions of the General Data Protection Regulation? https://www.lexology.com/library/detail.aspx?g=5ae76660-9770-4718-9010-6657a9351496#:~:text=Under%20the%20GDPR%2C%20individuals%20have,right%20to%20object%20to%20data

EU's General Data Protection Regulation (GDPR): Key Provisions and Best Practices - https://www.americanbar.org/groups/international_law/publications/international_law_news/2018/winter/eu-general-data-protection-regulation-gdpr/

Cyber Law of USA – https://www.asianlaws.org/gcld/gcld.php?country=US)
California Consumer Privacy Act (CCPA): What you need to know to be compliant; https://www.csoonline.com/article/3292578/california-consumer-privacy-act-what-you-need-to-know-to-be-compliant

Cyber Law of Singapore – https://www.asianlaws.org/gcld/gcld.php?country=SG)

MMC CYBER HANDBOOK 2021

India's Personal Data Protection Bill 2019, PWC Publication

Importance of Cyber Law In India - http://www.legalserviceindia.com/legal/article-1019-importance-of-cyber-law-in-india.html

India: Cybersecurity Comparative Guide - https://www.mondaq.com/india/technology/963026/

Cyber Space Jurisdiction: Issues and Challenges - https://www.legalbites.in/cyber-space-jurisdiction-issues-challenges

Cyber laws in India- http://iibf.org.in/documents/Cyber-Laws-chapter-in-Legal-Aspects-Book.pdf

Cybersecurity in India- https://www.lexology.com/library/detail.aspx?g=4cd0bdb1-da7d-4a04-bd9c-30881dd3eadf

Cyber Security and Their Laws in India: https://lawsisto.com/legalnewsread/NzAwNg==/Cyber-Security-And-Their-Laws-In-India#:~:text=Cyber%20laws%20deal%20with%20legal,are%20a%20part%20of%20cyberspace.&text=Cyberlaw%20is%20important%20because%20it,world%20wide%20web%2C%20and%20cyberspace

Legal Aspects of Cybersecurity - https://www.justitsministeriet.dk/sites/default/files/media/Arbejdsomraader/Forskning/Forskningspuljen/Legal_Aspects_of_Cybersecurity.pdf

2020 Data Breach Investigations Report – Verizon

Cyber Security Awareness for Citizens issued by Office of Special Inspector General of Police Maharashtra Cyber, Home Department, Government of Maharashtra

The biggest data breaches in India – https://www.csoonline.com/article/3541148/the-biggest-data-breaches-in-india.html#

Overview of Top Cybersecurity Breaches in India - https://www.firecompass.com/wp-content/uploads/2017/10/CyberSec-Breaches-in-India-Report.pdf

Top cybersecurity facts, figures and statistics for 2020 – https://www.csoonline.com/article/3153707/top-cybersecurity-facts-figures-and-statistics.html

Enhancing the Role of Insurance in Cyber Risk Management – https://www.oecd.org/daf/fin/insurance/Enhancing-the-Role-of-Insurance-in-Cyber-Risk-Management.pdf

Get insights into breach incidents by industry, source, type, and geographic region- https://www6.thalesgroup.com/breach-level-index-report-1H-2016-press-release

EIOPA Understanding of Cyber Insurance- https://www.eiopa.europa.eu/sites/default/files/publications/reports/eiopa_understanding_cyber_insurance.pdf

Ten Key Questions on Cyber Risk and Cyber Risk Insurance – https://www.genevaassociation.org/sites/default/files/research-topics-document-type/pdf_public/cyber-risk-10_key_questions.pdf

Various cyber insurance policy wordings including AIG, Hiscox, Beazely, TMK, Delta, Talbot, Bajaj Allianz, HDFC Ergo, ICICI Lombard

Business Interruption: The Unexpected Cost of a Cyber Incident
https://www.advisenltd.com/blog/cyber-tech-risk/business-interruption-the-unexpected-cost-of-a-cyber-incident/#:~:text=Another%20concept%20related%20to%20cyber,of%20a%20shared%20computer%20system.

Cyber Security –
https://niti.gov.in/sites/default/files/2019-07/CyberSecurityConclaveAtVigyanBhavanDelhi_1.pdf

When tech is the target: cyber risks for tech companies –
https://axaxl.com/fast-fast-forward/articles/when-tech-is-the-target_cyber-risks-for-tech-companies

Cybersecurity in Banking: Three Top Threat Trends to Know
https://securityscorecard.com/blog/cybersecurity-in-banking-three-top-threats-trends-to-know#:~:text=The%20banking%20industry's%20cyber%20threat,credentials%20when%20carrying%20out%20attacks.andtext=Vendors%20have%20access%20to%20critical,prime%20target%20for%20threat%20actors.

Top 5 Cyber Threats Facing Banks in 2020-
https://hubsecurity.io/top-5-cyber-threats-facing-banks/

Cyber Security Insiders- https://www.cybersecurity-insiders.com/upcoming-webinars/

Cyber risk in advanced manufacturing-
https://www2.deloitte.com/us/en/pages/manufacturing/articles/cyber-risk-in-advanced-manufacturing.html

How Cyber Insurance Is Beneficial For Manufacturing Industry?
https://medium.com/dataseries/how-cyber-insurance-is-beneficial-for-manufacturing-industry-e3c0719f9543

Indian manufacturing industry at high cyber security risk-
https://www.asianage.com/technology/in-other-news/290619/indian-manufacturing-industry-at-high-cyber-security-risk.html

Startups, SMEs most vulnerable in India to cyberattacks: Report
https://m.timesofindia.com/companies/startups-smes-most-vulnerable-in-india-to-cyberattacks-report/amp_articleshow/78831062.cms

With cyber-attacks on the rise, data of SMEs as the target, cyber insurance is the saviour

https://smefutures.com/cyber-attacks-on-the-rise-data-cyber-insurance-is-the-saviour/

A cyber security incident can be catastrophic for small businesses- https://m.economictimes.com/small-biz/sme-sector/a-cyber-security-incident-can-be-catastrophic-for-small-businesses/amp_articleshow/67995513.cms

DSCI Cyber Adoption Framework for SMBs- https://www.dsci.in/content/dsci-cyber-adoption-framework-smbs

The Bodily Injury & Property Damage Gap In E&O And Cyber Policies
https://www.gbainsurance.com/BIPD-Insurance-Tech-Cyber-717
Avoiding The Most Common Cyber Insurance Claim Denials
https://www.gbainsurance.com/avoiding-cyber-claim-denials

Cyber Pricing- https://www.actuaries.org.uk/documents/g2-pricing-workshop-cyber-pricing

The Changing Face of Cyber Claims
https://www.marsh.com/cy/en/insights/research-briefings/cyber-claims-report.html

Why AIG - What's Inside CyberEdge
https://www.aig.co.uk/content/dam/aig/emea/united-kingdom/documents/Financial-lines/Cyber/aig-cyberedge-whatsinside-0517-v5.pdf

Demystifying cyber insurance coverage:
https://www2.deloitte.com/content/dam/Deloitte/nl/Documents/financial-services/deloitte-nl-fsi-demystifying-cyber-insurance-coverage-report.pdf

Encouraging Clarity in Cyber Insurance Coverage The Role of Public Policy and Regulation: OECD

https://www.oecd.org/finance/insurance/Encouraging-Clarity-in-Cyber-Insurance-Coverage.pdf

Defamation in the Internet Age: Laws and Issues in India

https://blog.ipleaders.in/cyber-defamation-india-issues/#:~:text=Indian%20Penal%20Code&text=Section%20500%20of%20IPC%20provides,the%20reputation%20of%20a%20person.

Dealing with cyber accumulation risk

https://www.munichre.com/topics-online/en/digitalisation/cyber/dealing-with-cyber-accumulation-risk.html#:~:text=In%20terms%20of%20cyber%2C%20the,of%20a%20typical%20cyber%20policy

Managing cyber risks in an interconnected world

https://www.pwc.com/gx/en/consulting-services/information-security-survey/assets/the-global-state-of-information-security-survey-2015.pdf

MANAGING CYBER INSURANCE ACCUMULATION RISK

https://www.jbs.cam.ac.uk/wp-content/uploads/2020/08/crs-rms-managing-cyber-insurance-accumulation-risk.pdf

Swiss Re - Sigma - Cyber: getting to grips with a complex risk

https://www.swissre.com/dam/jcr:995517ee-27cd-4aae-b4b1-44fb862af25e/sigma1_2017_en.pdf

Cyber Risk Literacy and Education Index

https://www.oliverwymanforum.com/cyber-risk/cyber-risk-literacy-education-index.html#:~:text=The%20index%20assesses%2049%20geographies,knowledge%20through%20education%20and%20training