Report of the Working Group to study Cyber Liability Insurance

बीमा विनियामक और विकास प्राधिकरण

Insurance Regulatory and Development Authority of India

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

Respected Sir,

Subject: Working Group to study Cyber Liability Insurance – Report on Individual Cyber Insurance

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 the Working Group on Individual Cyber Insurance along with Model Policy wording.

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

Yours Sincerely,

Place: Hyderabad
Date: 23-11-2020

P. Umesh
Chairman of the Working Group

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

IRDAI Order of the Working Group

Working Group to Study Cyber Liability Insurance

-

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.

(Yegnapriya Bharath)
Chief General Manager (NL)

Table of Contents

Item	Subject	Page No.
	Executive summary	1
	Introduction	3
Chapter -1	Emergence of Cyber risk for individuals	5
Chapter -2	Cyber insurance policy -Coverage	7
Chapter -3	Need for individual cyber insurance	9
Chapter -4	Individual Cyber Insurance Cover – Salient features	13
Chapter -5	Gaps in the current covers and recommendations for improvements	15
Chapter -6	Standardisation of Cyber Insurance Policies – Challenges & Difficulties	17
Chapter -7	Suggestions to popularise Individual Cyber Insurance	19
Chapter -8	Suggested Dos and Don'ts for individual cyber insurance policy buyers	21
	References	23
	Annexure – Model Policy wordings	25

This page has been left blank

EXECUTIVE SUMMARY

Cyber risks permeate every aspect of our lives – whether it is for companies or individuals. These risks have become more pronounced in the post Covid-19 world. Rising incidences of cyberattacks and growing number of data breaches and digital infrastructure interruptions are visible in the country and around the world.

This report discusses the increasing exposures of individuals in the context of surge in usage of online services including online banking activities, digitization of records of personal and other information, extensive use of payment systems, significant growth in ecommerce, increase in the number of connected devices, extensive use of social media, relatively inadequate knowledge of cyber safety measures and the ubiquitous Coronavirus.

Cyber insurance policy is a risk transfer mechanism for cyber risks. Individual cyber insurance policy is the one which is designed to meet the requirements of an individual as against an organisation. Global survey conducted by Swiss Re reveals that Individuals are more worried about financial losses resulting from illicit access of financial credentials, identity theft, data loss due to technical issues and breach of privacy.

To protect customers from unauthorised transactions, Reserve Bank of India (RBI) has come out with guidelines limiting liability of customers in unauthorised electronic banking transactions including stipulating zero liability in certain situations. It may be noted that zero liability provision is not a *carte blanche*. Further, Cyber insurance addresses exposures beyond the situations described in RBI no. RBI/2017-18/15 dated July 6, 2017.

Salient features of individual cyber insurance include coverage in respect of Theft of funds, Identity theft, Social media exposures, Cyber stalking, Data restoration costs, Media liability, Cyber extortion and data and privacy breaches.

Cyber insurance policies, currently available, address the requirements of individuals reasonably well. But, there are some areas in the product features and processes which need improvement. Recommendations made to fill in the gaps include need for flexibility in insistence of an FIR at the time of claims, clarity in exclusion language relating to compliance with reasonable practices and precautions, targeted intrusion, unsolicited communication and the need for coverage for bricking costs etc.

Suggestions are made to popularise cyber insurance. These suggestions include brining about increased awareness about the policy, making the policy language and claim process easy to follow, give a fillip to group and affinity policies and allow bundling cyber cover with package policies etc.

While standardisation of Cyber insurance policy seems to be a good idea, 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.

Notwithstanding the above, insurers can build in certain minimum covers as a part of individual cyber insurance to facilitate better understanding in the market. A model policy wording, conceptualised by the Working Group, can be considered by the insurers as a reference point to provide minimum basic coverage.

It is good to advise customers about Dos and Don'ts with regard with regard to cyber security. The report lists the same for individual cyber insurance policy buyers which help spread awareness on cyber vulnerabilities and risk mitigation.

INTRODUCTION

We live in an ever-connected world today and every technology, every interface, every click we do on our devices (in some cases you don't even do anything e.g. connected homes) produces various forms of data. This is why many call it the information age quickly evolving into an age of artificial intelligence. Technology as we know is changing faster than ever and data is being generated at exponential rates. IBM estimates that about 90% of the data in the world today has been created in the last two years.

While the ability to capture data and putting it to right use benefits governments, corporations, institutions, science, social welfare and many others; more data also means vulnerability to data related risks & crimes. Every technology misuse, wrongful access or resulting losses are directly or indirectly about generation, storage, access and use of data. Digital data and technology related crimes are referred to as "Cyber Crimes".

India has been at the forefront of digital adoption driven by government impetus, infrastructural investments in communication, our need for remote connectivity and a vibrant technology driven industry. Our digital scale, spread, penetration and demographics are unique in many ways and aids our development. For example, India's smartphone base is estimated to reach 820 million in the next two years, which can unlock 80% improvement in efficiency and 8 times reduction in processing time for e-governance services. Initiatives like Digital India, the India stack, UID, RBI regulated UPI, etc have helped permeate digitisation in several aspects of our life, businesses, finances and work. Along with industry driven platforms for e-commerce, travel, health, banking, education, social media, etc; these digital solutions have become inseparable to our day to day life.

Every aspect of us from who we are (identity), what we do (work, travel, entertainment, etc), what & how we earn and transact (finances, payments, etc), what we communicate & consume as content (social media, internet, OTT platforms, etc), etc. is now interconnected. We are sharing, generating and consuming a lot of data and utilising data driven services in the process.

Looking at where we stand, it is hard to imagine that we are still in early stages of digital evolution and the immense potential a country like ours has to turn around its socioeconomic fortune & global status by leveraging digital data.

This page has been left blank

Chapter -1

Emergence of cyber risk for individuals

There is always an element of risk involved in all online activities. But the way individuals use online services, such as storing credit card details on a retailer's website or sharing sensitive personal data via an unprotected wireless network, or use of non-encrypted websites, they expose themselves to risks

When an individual's bank details are compromised or stolen it can be the start of a series of losses such as unlawful withdrawal of funds, identity theft, and such other losses.

Fraudsters may use personal information to open bank accounts or take out loans in victim's name. This will involve payment default notices and a damaged credit record all of which may only come to light several months after the fraud was perpetrated.

In case of identity theft, there might be emotional and psychological setbacks due to Cyberbullying and stalking. This is how our digital lives can start to impact on our overall wellbeing.

Impact of Covid–19

While everyone is focused on health and economic threats of the COVID 19 virus, cyber criminals around the world are taking it as an opportunity and capitalising on this crisis.

Cyber risks have accelerated by as much as 500% since the first lockdown was imposed in India in March 2020. There is an increase in coronavirus-themed spam, likely resulting in more infected personal computers and phones.

As per the national cyber security agency The Computer Emergency Response Team of India (CERT-In), there has been an increase in the number of cyber attacks on personal computer networks and routers since professionals were asked to work from home in the wake of the COVID-19 outbreak in the country.

- Cybercriminals are releasing new computing viruses and mobile applications relating to COVID-19 updates and other information.
- They are also designing phishing websites, emails and phishing UPI accounts in name of COVID-19, which are leading to Cyber frauds.
- They are using the heightened digital footprint and traffic to find vulnerabilities, or to siphon off money.
- They are launching Covid-19-themed attacks in the form of phishing emails with malicious attachments that drop malware to disrupt systems or steal data and credentials.

- They are creating temporary websites or taking over vulnerable ones to host malicious code. They lure people to these sites and then drop malicious code on their digital devices.
- Fake websites have also been soliciting donations for daily wage earners through email links.
- Some Covid-19 patient count-status apps and links are laden with viruses and identity theft malware.
- The bait websites pretending to be official government webpages have also resulted in major cyber frauds and have affected individuals severely.

The surge in communications and the wholesale shift to digitisation and to operate online have increased the risk of cyber-attacks by an order of magnitude.

The tendency towards adhoc decision making during crisis only accelerates the opportunity to infiltrate data. The awareness around the different forms of cybercrimes is in nascent stage in India and therefore, it is of prime importance to look at different scenarios that could be unfavourable and the methods of addressing various risks.

In the context of above, one of the risk transfer instruments available to individuals is Cyber Insurance.

Chapter -2

Cyber insurance policy - Coverage

Losses normally covered under a cyber-insurance policy can be split into 4 categories:

1. **First Party Losses**: Direct Financial Loss, Data recovery, Business Interruption Cover and Mitigation Costs Cover,

2. **Regulatory Actions**: Costs of Regulatory actions and investigations, Civil fines and penalties and Defence Costs.

3. **Crisis Management Costs**: Forensic Expert Cover including security consultation, Reputation Damage Cover, Legal Costs Cover for matters including notification, coordination with service providers, strategy etc., Credit and Identity Theft Monitoring Cover, Cyber extortion/ Ransomware Cover, Operation of a 24x7 Hotline, Cyber Stalking, Counselling, Information removal and pursuing action.

4. **Liability Claims**: Legal liability/damages directly arising from privacy or data/ security breach, Defamation, Intellectual Property Right (IPR) infringement and Defence Costs.

This page has been left blank

Chapter -3

Need for individual cyber insurance

What is Cyber Insurance?

Cyber insurance is an insurance policy designed to protect the policy holders from cybercrimes. Data Security Council of India **(DSCI**) describes cyber insurance as under

"Cyber Insurance is designed to guard businesses from the potential effects of cyber-attacks. It helps an organisation mitigate risk exposure by offsetting costs, after a cyber-attack/breach has happened. To simplify, cyber Insurance is designed to cover the fees, expenses and legal costs associated with cyber breaches that occur after an organisation has been hacked or from theft or loss of client/employee information.

Cyber Insurance is a risk management and mitigation strategy having a corollary benefit of improving the adoption of preventive measures (products, services, and best practices), thus, helping improve the cyber security posture of organisations, and thereby the country as well"

Individual cyber insurance policy is the one which is designed to meet the requirements of an individual as against an organisation. What are the big cyber worries for an individual?

As per Swiss Re's global survey, the top four cyber risk scenarios that people worry about most are:

1 illicit access of financial credentials (a hacker gets access to your online banking details and might therefore be able to steal money)

2 identity theft (an attacker steals your digital identity to purchase goods or services online in your name)

3 data loss due to a technical issue (your personal data gets deleted by a virus or software glitch)

4 illicit publication of personal data (somebody else publishes your private pictures online)

These are the four main areas where customers are receptive to the idea of a cyber insurance policy that will cover them against some of the consequences of these fears coming true.

In the Indian context, the following information about increased digitisation of transactions and internet usage would help understand the vulnerabilities and the resultant need for individual cyber insurance to mitigate the impact of adverse consequences.

- Government have taken many initiatives in order to spread the awareness of about digitisation of transactions, have encouraged individuals to avail digital facilities such as online portal to store personally identifiable information including health record and use payment system such as Rupay etc. It is possible that those portals may get breached and information obtained misused. As a result, individuals may face losses.

- The number of internet users in India is currently estimated at 700 million. India is ranked as the second largest online market worldwide in 2019, coming second only to China. The number of internet users is estimated to increase in both urban as well as rural regions. This number is increasing rapidly so also is the number of users of online banking.

- The number of online banking users is expected to reach 150 million by 2020 from 45 million in 2017.

- The Ecommerce industry is expected to reach $99 billion in size while the online retail penetration is expected to more than double to around 11% by 2024 from 4.7% in 2019.

- According to the Reserve Bank of India's (RBI's) settlement data of select payment systems, Unified Payments Interface (UPI) crossed 1 billion transactions in volume by mid-October 2020. With major e-commerce platforms conducting their festive sales with discounts and offers, experts believe that the growth of digital transactions will receive a further boost.

- The way many devices like computers, mobile phones, security systems, televisions, wearables connected to the internet are rapidly increasing, undoubtedly increases vulnerability of an individual for a cyber-attack. As per a study titled, "India - Emerging Hotbed of IoT Opportunities by Zinnov, a leading global management and strategy consulting firm, the number of connected devices will touch 2 Billion by 2021.In our increasingly connected world, the risk does not stop just because the systems are switched off.

- Also, it has been noticed that, there is an impactful increase in number of cybercrime targeting individuals. More than 90,000 case have been reported from 2012 till 2018. Out of 80% of them had intention of unlawful financial gain. In addition, it is believed that most of cyber frauds go unreported in India due to low level of consumer awareness, inadequate knowledge about recourse mechanisms and also because of individually insignificant losses (can be massive when looked at large).

- The use of social media has increased significantly in past few years across all classes in the society. Identity theft is a real threat to many social media users, as millions of online users use their personal information in order to get

registered with one or more social media platforms. Such huge information with personal data of so many people is one of the easiest targets for many cyber criminals. In addition to phishing emails and texts, social media is growing to be a major source of account access related frauds. Cybercrimes on social media include impersonation where a fake account is used to groom a victim, eventually tricking them into handing over money or representing another person through a fake identity.

- This risk is compounded by the fact that awareness & investment in cyber security measures like use of anti-viruses, firewalls, etc is limited. There is little awareness around use of privacy measures available on social medial platforms (e.g. public vs private posting), phone security (e.g. use of passwords & biometrics), etc.

- Some of the ways financial fraud can be perpetrated is through phishing or spoofing attacks, malware or spyware, SIM swap (original SIM gets cloned and becomes invalid, and the duplicate SIM can be misused to access the user's online bank account to transfer funds), credential stuffing (compromising devices and stealing data), man-in-the-middle attacks during online payments or transactions, identity theft, card cloners or readers at ATM machines and as simple as imposters calling up unsuspecting individuals and asking their personal banking details. The safety of bank accounts, and debit and credit card lies with the customer as well as the concerned bank. Taking the cognizance of the complaints related to unauthorized transactions, in July 2017, the RBI reviewed the criteria for determining customer liability in such cases and issued some directions. RBI has also set forth the situations to establish liability of a customer.

2) Zero Liability of a customer

- ✓ Contributory fraud/ negligence/ deficiency on the part of the bank, irrespective of whether or not the transaction is reported by the customer

- ✓ Third party breach where the deficiency lies neither with the bank nor with the customer but lies elsewhere in the system, and the customer notifies the bank within 3 working days of receiving the communication from the bank regarding the unauthorized transaction

3) Limited Liability of a customer

- ✓ Where loss is due to the negligence of the customer, e.g. payment credentials are shared, the customer shall bear the entire loss till the time unauthorized transaction is reported to the bank. Any loss after reporting of the unauthorised transaction shall be borne by bank.

- ✓ In cases where the responsibility for the unauthorised electronic banking transaction lies neither with the bank nor with the customer, but lies elsewhere in the system and when there is a delay (of four to seven working days after receiving the communication from the bank) on the part of the customer in notifying the bank of such a transaction, the per transaction liability of the customer shall be limited to the transaction value or the amount ranging between INR 5,000 to INR 25,000 whichever is lower dependent upon the type of account.

Detailed directions are in RBI circular no. RBI/2017-18/15 dated July 6, 2017.

It may be noted that Zero liability is not a *carte blanche*. Further, Cyber insurance addresses exposures beyond the situations described in RBI circular as per descriptions given in the later paragraphs.

Chapter -4

Individual Cyber Insurance Cover - Salient features

Given below are the salient features of individual cyber insurance policy.

1. **Theft of funds –** Provides protection in respect of theft of funds due to Cyber Incident or Hacking of insured's Bank account, Credit/Debit card and/ or Mobile wallets by a Third Party.

2. **Identity Theft Cover –** Provides protection in terms of Defence cost for claims made against insured by third / affected party due to identity theft fraud, provides expense to prosecute perpetrators and other transportation cost.

3. **Social Media Cover / Personal Social Media-** Provides protection in terms of Defence cost for claims made against insured by third / affected party due to hacked social media account of insured, provides expense to prosecute perpetrators and other transportation cost.

4. **Cyber Stalking / Bullying** – Provides expenses to prosecute the stalker.

5. **Malware Cover / Data Restoration Cost** – Provides coverage for data restoration cost due to malware.

6. **Phishing Cover** – Provides protection in respect of financial losses as a result of phishing attack and provides expense to prosecute perpetrators.

7. **Unauthorised Online Transaction –** Provides protection against fraudulent use of bank account, credit / debit card, e-wallet by third party to make online purchasing over internet.

8. **Email Spoofing** - Provides protection in respect of financial losses as a result of spoofed email attack and provides expense to prosecute perpetrators.

9. **Media Liability Claims Cover** – Provides coverage for defence costs in third party claims due to defamation or invasion of privacy due to Insured's publication or broadcasting of any digital media content.

10. **Cyber Extortion Cover** – Provides protection for extortion loss as a result of Cyber extortion threat and provides expense to prosecute perpetrators.

11. **Data Breach and Privacy Breach Cover** – Provides indemnity for defence costs and damages in respect of claims lodged by a Third party against the Insured for Data Breach and or Privacy Breach

Chapter -5

Gaps in the current covers and recommendations for improvements

While the current offerings are addressing the requirements of individuals reasonably well, there are a few gaps which are listed below. Some of them relate to product features and the others to processes involved.

The working group feels that it may not be possible to address all these gaps. But, attempts can be made, in respect of some gaps, either to respond fully or partially.

S. No.	Gaps	Recommendations
1	Compulsory FIR in case of a Cyber incident is a must while filing a claim which becomes a hassle for an individual and creates distrust in their minds when claims are not settled because of the same	FIRs is a critical requirement to assess claims and hence can't be fully dispensed with. However for small claims upto INR 5000, Insurers may build flexibility with regard to this requirement
2	Individuals are required to take due diligence, care and reasonable precautions to safeguard their identity/personal details while on web and claims are admissible only if the Individual is an innocent victim of the cyber fraud and Gross negligence is excluded from the coverage. This again creates a grey area in the coverage	More explicit exclusion language could be used, e.g. - 'Deliberate, criminal, fraudulent, dishonest or malicious act or omission of Insured Beneficiary' Also, such exclusion should be triggered only when the said negligence has directly caused the loss
3	Definition of Cyber-attack states targeted intrusion into the Individual's system which is mostly not the case. The attack is usually targeted to multiple web users/content users and the said condition again leaves the Individual uninsured.	Insures could use "unauthorized access" language as suggested in the model policy form
4	Territory and Jurisdiction is restricted to India only in most of the policies. A number of syndicated frauds originate from outside India (e.g. phishing, ransomware, malware attacks), cyber insurance clauses may or may not be clear on the coverage in this regard.	Insurers may offer options for Worldwide territory. Jurisdiction for claims settlement should be India

5	Unsolicited communications are also excluded from the scope of cover in many insurance policies while this is one of the major reasons of cyber related losses leaving the individual uninsured.	Insurers could offer coverage for such losses
6	Sim-jacking, card cloning, skimming coverage is not available currently in the market while the same is a major reason of loss in India.	Insurers could offer coverage for such losses
7	Online shopping fraud like when the item that individual bought but not received the goods or sold, something that has left their custody but the payment is not received is not covered or only a very small coverage for the same is available	Insurers could offer coverage for such losses
8	Bricking: Cyber insurance policies generally exclude coverage for damaged computer hardware. Bricking refers to a loss of use or functionality of hardware as a result of a cyber-event. While malicious software may be removed, hardware may also require replacement. Here, coverage provides for the cost to replace such affected hardware.	Insurers could offer coverage for such losses

Chapter -6

Standardisation of Cyber Insurance Policies- Challenges & Difficulties

1. Cyber threats are growing and are dynamic, cyber threat actors adopt new technologies faster and exploit it to their benefit, and hence cyber insurance as a risk transfer method should also be dynamic and continue to respond to latest developments.

2. New legislation and regulations are in development and this may lead to requirement of new insurance solutions and services.

3. Cyber experts, insurers and reinsurers are learning and trying to develop better understanding on exposures and insurance solutions. Policy wording, coverage and offerings are getting refined however, this is still a long journey.

4. The user base is across all age groups, be it enthusiastic young kids & young adults who are on internet for school education and other social networking sites to explore internet services much aggressively; the professionals having much more dependence on internet for day to day business. Another set of users are the elderly in form of parents and grandparents who have also joined the enthusiastic user segment. Each of these segment faces very different level of threats like Cyber bullying or Harassment, to Data theft or Malware attack to Digital theft of funds and Identity theft. This is a very wide spectrum to be addressed by a standard product and needs a flexible approach.

5. It appears that no other market has standardized yet the wordings as it is not considered desirable from customer's perspective. Flexibility allows for innovation and healthy competition, and not just price driven competition.

6. 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 development in the market.

7. To increase penetration of the product various distribution channels have to be used and this will require flexible approach in coverage and services. It is good to allow market to explore, innovate and invest in the product proposition along with various risk management services.

As mentioned above, Cyber insurance product is in a development phase, and standardisation of the Cyber policy wordings for individuals may hamper the

developments of this product in Indian market. It is important now to focus on popularizing the Cyber insurance product, make it easier for insurer to adapt the product as per the customer requirements and continue to enrich customer's experience and protection.

In view of the foregoing, the working group feels, it is neither desirable nor possible to standardise the cover at this juncture. Nevertheless, Insurers can build in certain minimum covers as a part of individual cyber insurance. The attached model policy wording can be considered by the insurance industry as a reference point to provide minimum basic coverage.

Chapter -7

Suggestions to Popularise Individual Cyber Insurance

Individual cyber insurance was introduced in India sometime in 2017. While a few insurers have filed this policy with IRDAI, it has not gained much traction so far. The following are some suggestions to popularise individual cyber insurance policy.

1. Awareness Campaign: Awareness about the policy is currently low. Insurance industry should launch awareness campaign to educate consumers about their exposures and the insurance protection available to mitigate the losses

2. Policy wording must be easy to understand and claim process must be easy to comprehend and implement

3. Dissemination of information about claim scenarios/ settlements without confidentiality breaches.

4. Group policies, including affinity policies, may be encouraged as the reach of the message gets wider

5. Insurers may consider offering cyber insurance as a part of package policy like House Holders Package policy. Swiss Re's global survey reveals that many would prefer to buy personal cyber insurance in combination with other products

6. It is better to offer a base version of the policy at an affordable premium and then give the customer an option to choose additional covers

This page has been left blank

Chapter -8

Suggested Dos and Don'ts for individual cyber insurance policy buyers

Do's

1. Install Anti-Virus and Firewall in devices
2. Use a Virtual Private Network
3. Keep software and operating system updated
4. Keep hard-to-Guess Passwords or Passphrases, Password should have a Minimum of 10 Characters using uppercase letters, lowercase letters, numbers and Special Characters
5. Keep different passwords for different accounts. If one password gets hacked, your other accounts are not compromised
6. Use Privacy Settings On Social Media Sites to Restrict Access To Your Personal Information
7. Pay Attention to Phishing Traps in Email and watch for Telltale Signs of a Scam
8. Destroy Information Properly When It Is No Longer Needed
9. Be Aware of Your Surroundings When Printing, Copying, Faxing or Discussing Sensitive Information.
10. Lock your Computer and mobile phone when not in use. This Protects Data from Unauthorized Access and use
11. Remember that wireless is inherently insecure. Avoid using public wi-fi Hotspots
12. Report all suspicious activity and cyber incidents
13. Check if the web site being visited is a trusted web site
14. Be extra careful during festival season
15. Always delete mail/ SMS from unknown sources

Don'ts

1. Leave or share your sensitive information lying around or share to some one
2. Share or post any private or sensitive information, such as credit card numbers, passwords or other private information, to some one, on public sites, including social media sites
3. Click on links from an unknown or untrusted source

4. Respond to fake phone calls or emails requesting for confidential data
5. Install Unauthorized Programs on your computer
6. Leave devices unattended. Keep all mobile devices, such as laptops and cell phones physically secured
7. Share personal information with persons unless authenticity and required authority is confirmed

References

1. https://www.mckinsey.com/business-functions/mckinsey- digital/our-insights/digital-india-technology-to-transform-a-connected-nation
2. https://www.statista.com/statistics/255146/number-of-internet-users-in-india/#:~:text=Number%20of%20internet%20users%20in%20India%202015%2D2025&text=In%202020%2C%20India%20had%20nearly,for%20the%20south%20Asian%20country.
3. https://digitalindia.gov.in/content/online-banking-users-reach-150-billion-2020
4. https://www.ibef.org/industry/ecommerce-presentation
5. https://www.financialexpress.com/industry/banking-finance/online-banking-users-in-india-to-reach-150-billion-by-2020-according-to-a-study/731048/
6. https://www.webhostingsecretrevealed.net/blog/ecommerce/online-shopping-ecommerce-and-internet-statistics-2020-you-should-know/#:~:text=79%25%20of%20smartphone%20users%20have,in%20mobile%20page%20load%20time.
7. https://www.businesstoday.in/current/corporate/indias-ecommerce-industry-goldman-sachs-survey-online-shopping-grocery-ril/story/411139.html#:~:text=India's%20e%2Dcommerce%20industry%20is,of%20e%2Dcommerce%20markets%20globally.
8. https://www.businesstoday.in/current/corporate/indias-ecommerce-industry-goldman-sachs-survey-online-shopping-grocery-ril/story/411139.html#:~:text=India's%20e%2Dcommerce%20industry%20is,of%20e%2Dcommerce%20markets%20globally.
9. https://www.statista.com/statistics/309435/india-cyber-crime-it-act/#:~:text=From%202012%20to%202018%2C%20there,than%20121%20percent%20since%202016.
10. https://economictimes.indiatimes.com/wealth/personal-finance-news/cyber-criminals-stole-rs-1-2-trillion-from-indians-in-2019-survey/articleshow/75093578.cms?from=mdr
11. https://trak.in/tags/business/2020/10/19/1-billion-upi-transactions-worth-rs-1-9-trillion-in-15-days-upi-grows-100-in-1-year/
12. https://www.facebook.com/IBM/posts/90-of-the-data-in-the-world-today-has-been-created-in-the-last-two-years/293229680748471/
13. https://economictimes.indiatimes.com/industry/telecom/telecom-news/indian-to-have-820-million-smartphone-users-by-2022/articleshow/76876369.cms?from=mdr
14. RBI circular no. RBI/2017-18/15 dated July 6, 2017.
15. Swiss Re - White Paper Personal cyber insurance: Protecting our digital lives
16. CYBER INSURANCE IN INDIA - Mitigating risks amid changing regulations & uncertainties - Data Security Council of India (DSCI) – A NASSCOM initiative

This page has been left blank

ANNEXURE:

Individual Cyber Insurance Policy

Model Policy Wording

IRDAI WORKING GROUP TO STUDY CYBER LIABILITY INSURANCE
18th November 2020

Table of Contents

Sl. No	Particulars	Page No.
A	PREAMBLE	27
B	INSURING CLAUSE	27
i.	Theft of Funds/ Financial Loss Cover	27
ii.	Malware Decontamination Cover/ Data Restoration Cover	27
iii.	Cyber Extortion Cover	27
iv.	Cyber Stalking Cover	28
v.	Identity Theft Cover	28
vi.	Privacy Breach and Data Brach Cover	28
vii.	Media Liability Cover	28
C	DEFINITIONS	29
D	GENERAL CONDITIONS	34
E	SPECIAL CONDITIONS	36
F	EXCLUSIONS	37
G	DUTIES OF THE INSURED	38
H	CLIAM REPORTING / PROCESS	39
I	DEFENCE SETTLEMENT AND CLAIM COOPERATION	40
J	GRIEVANCE REDRESSAL MECHANISM	40

A. PREAMBLE:

Mr./Mrs./Ms. _____ (henceforth referred to as the "Insured") has submitted a proposal and declaration.

---------- (henceforth referred to as "Insurer"), relies on the information furnished in the proposal and declaration for this Policy, or its preceding Policy of which this is a renewal. On such reliance and in consideration of the premium received, the Insurer hereby agrees to the following Terms and Conditions. These Terms and Conditions will be the basis for any claim or benefit under this Policy.

B. INSURING CLAUSE:

In consideration of the payment of the premium, the Insurer and the Insured agree as follows:

i. Theft of Funds / Financial Loss Cover:

The Insurer shall indemnify the Insured during the Period of Insurance or Discovery Period
Any direct and pure financial loss sustained by the Insured:

(i) as a result of a theft of funds due to an unauthorized access to Insured's bank account, credit or debit card or mobile wallets by a third party, and

(ii) as a consequence of Insured being a victim of cybercrime - including but not limited to phishing, email spoofing, Vishing/ Hacking/ Skimming/ Smishing / Card Cloning/SIM Jacking.

ii. Malware Decontamination cover / Data Restoration Cover

The Insurer shall indemnify the Insured during the Period of Insurance or Discovery Period any reasonable and necessary costs incurred by the involvement of an IT expert after a cybercrime to restore insured's data or to decontaminate or clean insured's personal device from malware. Costs shall include Bricking costs.

iii. Cyber Extortion Cover

The Insurer shall indemnify the Insured during the Period of Insurance or Discovery Period
the Cyber Extortion Loss that the Insured incurs solely and directly as a result of a Cyber Extortion Threat first Discovered during the Period of insurance. As a condition for payment under this cover the Insured shall:

i. keep the terms and conditions of this Cyber Extortion Cover confidential, unless disclosure to law enforcement authorities is required; and
ii. Take all reasonable steps to notify and cooperate with the appropriate law enforcement authorities; and
iii. Take all reasonable steps (including the involvement of a security consultant with the Insurer's prior written consent), to effectively mitigate the Cyber Extortion Loss.

iv. Cyber Stalking Cover

The Insurer shall indemnify the Insured during the Period of Insurance or Discovery Period if applicable Costs incurred by the Insured for prosecution of a criminal case against Third party under The Information Technology Act 2000 (No 21 of 2000), and or any other applicable law prevalent in India including the relevant provisions of Indian Penal code for Cyber Stalking the Insured.

v. Identity Theft Cover

The Insurer shall indemnify the Insured during the Period of Insurance or Discovery Period if applicable all Defense Costs incurred as a result of any Claim by an Affected Person or an entity for Legal liability that directly results from the Identity Theft of the Insured by Cybercrime .

vi. Data Breach and Privacy Breach Cover

The Insurer shall indemnify the Insured during the Period of Insurance or the Discovery period if applicable, all Defence Costs and damages lodged by a Third party against the Insured for Data Breach and or Privacy Breach.

vii. Media Liability Cover

The Insurer shall indemnify the Insured during the Period of Insurance or the Discovery period if applicable, all Defence Costs and damages lodged by a Third party against the Insured for any unintentional

- defamation,
- breach of copyright, title, slogan, trademark, trade name, service mark, service name or domain name, or
- breach or interference of privacy rights,

resulting from Insured's online media activities including media activities in social media.

PROVIDED always that the liability of the Company shall in no case exceed the Limit of Liability stated against each item or in aggregate as stated in the schedule.

C. DEFINITIONS

In this Policy the following words in bold shall have the following meaning:

1. **Affected Person**: means any natural person who has been affected by the named insuring clauses
2. **Bricking costs** refer to costs incurred to repair/ replace hardware, where loss or impairment of functionality of hardware is caused by a Cybercrime. Bricking costs shall also include costs for removal of malicious software.
3. **Claim** means any written demand, suit or civil legal proceeding. A Claim shall be deemed to be first made or commenced when the Insured first becomes aware of it.
4. **Computer** means any electronic magnetic, optical or other high-speed Data processing device or system which performs logical, arithmetic, and memory functions by manipulations of electronic, magnetic or optical impulses, and includes all input, output, processing, storage, Computer software, or communication facilities which are connected or related to the Computer in a Computer system or Computer network;
5. **Computer Programs** means a collection of instructions that describe a task, or set of tasks, to be carried out by a Computer System, including application software, operating systems, firmware and compilers.
6. **Computer System** means a device or collection of devices, including input and output support devices and excluding calculators which are not programmable and capable of being used in conjunction with external files, which contain Computer Programmes, electronic instructions, input Data and output Data, that performs logic, arithmetic, Data storage and retrieval, communication control and other functions; For avoidance of Doubt, Computer System shall include all kinds of digital devices.
7. **Cybercrime** means an unauthorised intrusion into the Insured's Computer System:

   which results in the transmission of unauthorised Data to the Insured's Computer System or from the Insured's Computer System to a Third Party's Computer System that is designed to modify, alter, damage, destroy, delete, record or transmit information without authorisation, including Data that is self-replicating or self-propagating, or is designed to contaminate other Computer Programmes or legitimate Computer Data, consume Computer resources or in some fashion usurp the normal operation of a Computer System.

8. **Cyber Stalking** means the repeated use of electronic communications to harass or frighten someone.
9. **Cyber Extortion Threat** means threat by an extortionist to cause harm or damage to Insured's data on Insured's personal device in order to extract an extortion ransom by use of coercion.
10. **Cyber Extortion Loss** means:
    a) Reasonable and necessary fees, Costs and expenses incurred by or on behalf of the Insured with the prior written consent of the Insurer directly resulting from a Cyber Extortion Threat;
    b) Monies payable by the Insured with the prior written consent of the Insurer in order to resolve or terminate a Cyber Extortion Threat.

11. **Credit card cloning** is a technique whereby someone obtains an individual's credit card details, copies them onto a bogus card and begins using the credit card.

12. **Damages** means the following, incurred as a result of a Claim:
    i. any amounts that an Insured shall be legally liable to pay to a Third Party in respect of judgments or arbitral awards rendered against an Insured;
    ii. monies payable by an Insured to a Third Party pursuant to a settlement agreement negotiated by the Insured with the prior written approval by the Insurer; or
    iii. Civil fines and penalties, Punitive or exemplary Damages where insurable by the law of this Policy and the jurisdiction in which the payment is to be made.

    Damages shall not include:
    i. the loss, offset or return of fees, commissions, royalties, bonuses or profits by the Insured or the Costs to re perform any services;
    ii. the Costs to comply with any order for, grant of or agreement to provide injunctive or other non-monetary relief;
    iii. the Costs to design, upgrade, maintain, or improve a Computer System or Computer Programme, including correcting any deficiencies or problems;
    iv. Taxes
    v. Compensatory Costs.
    vi. Consequential Loss.
    vii. Cash Back/Reward points

13. **Data** means any electronic Data of a form readily usable by a Computer Programme.

14. **Data Breach and Privacy Breach** means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or

access to, personal data or confidential information transmitted, stored or otherwise processed on Insured's personal devices

15. **Data Protection Legislation** means any Law or Regulation regulating the processing of personal information, including the Indian Data Privacy Act 2019, Indian Information Technology Act, 2000 and Information Technology,(reasonable security practices and procedures and sensitive personal Data or information) Rules, 2009/2011 or any amendments or modifications thereof, from time to time or any similar legislation.

16. **Deductible** means the amount as mentioned in the schedule that the Insurer deducts from the covered loss before effecting payment.

17. **Defence Costs** means reasonable and necessary legal fees, Costs and expenses incurred by or on behalf of the Insured, with the prior written consent of the Insurer, in relation to the investigation, response, defence, appeal or settlement of a Claim, including the Costs of attachment or similar bonds, provided the Insurer shall have no obligation to furnish such bonds.

18. **Direct Financial Loss** shall mean the loss of funds belonging to the Insured as a Consequence of the Insured being an innocent victim due to Cybercrime

19. **Discovery Period** means the period commencing immediately after the expiry of the Period of Insurance, during which written notice may be given to the Insurer of a Claim arising from an insuring clause that has occurred prior to the expiry date of the Period of Insurance and only where Loss from such insuring clause is not partially nor wholly covered by any other insurance policy in force after the expiry date of the Policy.

20. **E-mail Spoofing** means a forgery or a wrongful manipulation of an E-mail header so that the message appears to have originated from the actual source.

21. **Financial Institution** means any bank whose function or principle activities are regulated by the Indian financial regulatory bodies in the territories in which it operates.

22. **Funds** mean any cash, money currency owned by the Insured or held by
    a) A Financial Institution
    b) A Payment System Operator in an Electronic form on behalf of the Insured.

22. **Hacking** is an attempt to exploit a computer system or a private network inside a computer system. It is an unauthorised access to or control over computer network security systems for some illicit purpose.

23. **Identity Theft** means any fraudulent and Unauthorized Access to, usage, deletion or alteration of Insured's Personal Data stored in the Insured's Computer System

24. **Insured** means the Policy Holder named in the Policy schedule.

25. **Insurer/ Company** means _____

26. **Insured's Computer System** means a Computer System the Insured leases, owns or operates and which is securely made available or accessible to the Insured for the sole purpose of storing and processing the Insured 's Data and which is not accessible for the general public

27. **Loss** means
    a) Direct financial loss
    b) Damages
    c) Defence Costs
    d) Restoration Costs
    e) Cyber Extortion Loss
    f) Consultant Costs
    g) Any other amount the Insurer is liable to pay under the terms and conditions of this Policy

28. **Malware** means a Computer program received through SMS, File transfer, downloaded programs from internet or any other digital means by the Insured's Computer System maliciously designed to infiltrate and damage Insured's Computer System without Insured's consent.

29. **Payment System Operator** is an entity authorized by the Reserve Bank of India to set up and operate in India under the Payment and Settlement Systems Act, 2007

30. **Phishing** is the attempt to obtain sensitive information such as usernames, passwords, and credit card details (and sometimes, indirectly, money), often for malicious reasons, by masquerading as a trustworthy Entity in an electronic communication

31. **Personal Data** shall mean any information or details such as bank details, photographs, name, location data etc. which are unique to an Individual and are stored in the Insured's Computer System.

32. **Policy Period:** means the period mentioned in the schedule not exceeding 12 months.

33. **Pollution** means the discharge, dispersal, seepage, migration, release or escape of:
    a) any solid, liquid, gaseous, biological or thermal irritant or contaminant, including smoke, vapor, soot, fumes, acids, alkalis, chemicals, radiation and waste. Waste includes materials to be recycled, reconditioned or reclaimed;
    b) electromagnetic energy, radiation or fields;
    c) nuclear or other radiation.

34. **Proposal Form** means the written application or proposal for this Policy made by the Policyholder, including any document provided by the Policyholder in connection with such application or proposal which shall be incorporated in and form the basis of this Policy.

35. **Regulator** means any official or public body with responsibility to enforce Data Privacy Regulation 2019 or Authority empowered to adjudicate the disputes/complaints, including but not limited to any Controller of Certifying Authorities, Deputy Controller of Certifying Authorities, Assistant Controller of Certifying Authorities, adjudicating officer, Cyber Appellate Tribunal, appointed or constituted under the Indian Information Technology Act, 2000 read with Information Technology (Reasonable security practices and procedures and sensitive personal Data or information) Rules, 2011, or such other Regulator/adjudicating authority as may be designated/appointed, from time to time.

36. **Restoration Cost** includes Reasonable and necessary Cost to technically restore, retrieve or reinstall Data or Computer Program damaged by entry of the Malware including the Cost of purchasing a Software License necessary to reproduce such Data or Computer Programs if so required to bring back to the position before occurrence of the incident excluding any improvement cost.

37. **Skimming** is a method used by identity thieves to capture information from a cardholder. Several approaches can be used by fraudsters to procure card information with the most advanced approach involving a small device called a **skimmer.**

38. **Smishing** is a portmanteau of "SMS" (short message services, better known as texting) and "phishing." When cybercriminals "phish," they send fraudulent emails that seek to trick the recipient into opening a malware-laden attachment or clicking on a malicious link. Smishing simply uses text messages instead of email.

39. **Social Media** means any forms of electronic communication (as Web sites for social networking and microblogging) through which users create online

communities to share information, ideas, personal messages, and other content (as videos)

40. **Third Party** means any natural or legal person except the Insured

41. **Vishing** is an attempt where fraudsters try to seek personal information like Customer ID, Net Banking password, ATM PIN, OTP, Card expiry date, CVV etc. through a phone call.

42. **Insured** means the Policy Holder named in the Policy schedule.

43. **Insurer** means ----- General Insurance Company Limited

44. **Unauthorized Access** or Use means the improper access or use of the Insured's Computer System by an unauthorized person acting in an unauthorized manner

D. GENERAL CONDITIONS:

1. **Limit of Liability:**
   The Insurer's liability to pay or indemnify under this contract for each and every Loss and for all Loss in the aggregate shall not exceed the Limit of Liability during the policy period

2. **Discharge of Insurer from Liability:**
   The payment of any Loss and or any other amounts payable under this Policy to the Insured shall fully release the Insurer from the Insurer's liability to make payment with respect to such Loss and all other amounts

3. **Policy Renewal:**
   The Insurer shall not be bound to accept any renewal premium nor give notice to the Insured that such renewal is due. No receipt for renewal premium is valid except on the official form issued by the Company. Under normal, circumstances renewal will not be refused except on the grounds of misrepresentation, fraud and non-disclosure of material facts or non-cooperation of the insured.

4. **No Third Party Rights:**
   Notwithstanding what is stated in any Law, this Policy is not intended to confer any rights or benefits on and or enforceable by any Third-Party other than an Insured and accordingly no Third Party shall acquire any rights in relation to or under this Policy nor can enforce any benefits or Claim under term of this contract against the Insurer.

5. **Assignment:**
   The Insured shall not be entitled to assign this Policy nor any interest or right under the Policy without the Insurer's prior written consent

6. **Contribution**:
   If at the time of any loss or damage happening to any property hereby insured there be any other subsisting insurance or insurance whether effected by the Insured or by any other person or persons covering the same risk, the Insurer shall not be liable to pay or contribute more than its rateable proportion of such loss or liability.

7. **Subrogation:**
   The Insured and any claimant under this policy shall at the expense of the company do or concur in doing or permit to be done all such acts and things that may be necessary or reasonably required by the company for the purpose of enforcing any rights and remedies or obtaining relief or indemnity from other parties to which the company shall be or would become entitled or subrogated upon the company paying for or making good any loss or damage under this policy whether such acts and things shall be or become necessary or required before or after the insureds' indemnification by the company. The Insurer reserves the right to recover amount due from any third party by virtue of Letter of Subrogation post settlement of the claim. Any amount recoverable from any Third party shall be sum payable to the insurers post settlement of the claim.

8. **Fraud:**
   If any claim under this policy shall in any respect be fraudulent or if any fraudulent means or devices are used by the insured or anyone acting on the insureds' behalf to obtain any benefit under this policy, all benefits and rights under this policy shall be forfeited and the policy will be null & void.

9. **Misrepresentation**:
   This policy shall be void in the event of mis-representation, mis-description or non-disclosure of any material particulars.

10. **Cancellation:**
    The Insurer may at any time, cancel this policy by giving seven (07/ 15) days' notice in writing by registered post or by courier to the Insured at his last known address in which case the Company shall return to the insured a proportion of the last premium corresponding to the un-expired period of insurance.

11. **Arbitration:**
    If any dispute or difference shall arise as to the quantum to be paid under the policy (liability being otherwise admitted) such difference shall independently of all other questions be referred to decision of a sole arbitrator to be appointed in writing by the parties to or if they cannot agree upon a single arbitrator to be appointed in writing by the parties to or if they cannot agree upon a single arbitrator within 30 days of any party invoking arbitration the same shall be

referred to a panel of three arbitrators, comprising of two arbitrators, one to be appointed by each of the parties to the dispute/difference and the third arbitrator to be appointed by such two arbitrators and arbitration shall be conducted under and in accordance with the provisions of the Arbitration and Conciliation Act, 1996.

It is clearly agreed and understood that no difference or dispute shall be referable to arbitration as herein before provided, if the company has disputed or not accepted liability under or in respect of this policy.

It is hereby expressly stipulated and declared that it shall be a condition precedent to any right of suit upon this policy that award by such arbitrator/arbitrators of the amount of the loss or damage shall be first obtained."

12. **Observance of Terms and Conditions**:
The premium payable under this policy shall be paid in advance. No receipt for premium shall be valid except on the official form/official website of the company. The due payment of premium and observance and fulfilment of the terms, conditions and endorsement of this policy by the insured shall be a condition precedent to any liability of the company to make any payment under this policy. No waiver of any terms, provisions, conditions and endorsement of this policy shall be valid unless made in writing and signed by an authorized official of the company. Any violations of terms & conditions will make the policy voidable at the option of the insurer depending on the degree of implication on the loss occurred, recovery prospects & investigation except in case of fraud & misrepresentation.

E. SPECIAL CONDITIONS:

1. The debit card/ credit card involved must be blocked immediately within 24 hours after detection of the loss of money or loss of card, which ever happens earlier.
2. Any cashback/rewards if so credited to the concerned card holder's account against misused transaction leading to loss of money, shall be reduced from the loss payable under the policy.
3. Insured should have a registered valid mobile number &e-mail id to receive SMS alerts/OTP from the bank.
4. This insurance shall not cover losses that can be received from a financial institution, payment wallet/service operator, ecommerce service provider or any such entity who has a primary responsibility to indemnify the insured.

F. EXCLUSIONS:

No coverage will be available under this Policy with respect to any Loss arising out of, based upon or attributable to:

1. **Dishonest and Intentional mis-conduct:**
   Any deliberate, criminal, fraudulent, dishonest or malicious act or omission; or intentional or willful violation of any duty, obligation, contract, law or regulation; by the Insured.

   Such acts should have directly caused the loss for the exclusion to apply.

   Provided, however, the Insurer shall advance Defense Costs until there is
   a) final decision of a court, arbitration panel or Regulator, or
   b) a written admission which establishes such behavior. Following such finding the Insurer shall be entitled to repayment of any amount paid to or on behalf of the Insured under this Policy.

2. **Bodily Injury:**
   Any actual or alleged bodily injury, sickness, mental anguish or emotional distress or disturbance, disease or death of any person howsoever caused.
3. **Property Damage:**
   Any damage to or destruction of any property, including loss of use thereof.
4. **Contractual Liability:**
   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;
5. **Prior Acts Exclusion:**
   Any Claim due to, arising out of or based upon or attributable to acts committed, attempted, or allegedly committed or attempted, prior to the inception of the coverage and known to the Insured
6. **Intellectual Property Rights:**
   Any actual or alleged plagiarism or infringement of any Trade Secrets, patents, trademarks, trade names, copyrights, licenses or any other form of intellectual property.
7. **Trading:**
   Any losses or liabilities connected with any types of purchase or sale transactions or other dealing in securities, commodities, derivatives, foreign or Federal Funds, currencies, foreign exchange, cryptocurrencies and the like.

8. **Outage/Disturbance Loss:**

Losses due to the outage/disturbance of external networks (e.g. power, internet, cable & telecommunications)

9. **Commercial, Political, Union or Religious Activities:**
   Any kind of losses in connection to commercial, political or union activities, the exercise of a religious function/office and/or the membership in any club/association that is salaried and/or not for leisure.

8. **Immoral/Obscene Services:**
   Any losses in connection with racist, extremist, pornographic or other immoral/obscene services, statements or representations provided made or committed by the insured.
9. **Professional Services:**
   Any loss or damage attributable to rendering or non-rendering of professional services
10. **Sharing/Divulging user id and password:**
    Any sharing of divulging of id / password leading to loss of money/data.
    Any act of error and commission by insured causing over payment or transfer to a wrong bank account not intended to.
11. **Loss of Reputation/Goodwill**
12. **Matters uninsurable by law.**
13. **Prior/ Pending Litigation:**
    Any legal proceedings which commenced prior to inception of this policy
14. **War & Terrorism**
    Any actual, threatened or feared act of:
    a) war, invasion, act of foreign enemy, hostile operations (whether war has been declared or not), civil war, rebellion, revolution, insurrection, riot or civil commotion, military or usurped power or martial law, or

    b) Violence or other intended harm to human life or health or to property for political, religious or other ideological reason and for the purposes of intimidating, coercing or harming, in part or in whole, any government, population or segment of economy, except to the extent exclusively carried out through an actual Cybercrime.

G. DUTIES OF THE INSURED:

Insured shall take all reasonable measures to safeguard the Insured's Computer System and Digital Devices and prevent the occurrence and to minimize the impact of any Cybercrime including but not limited to

i. Updating Antivirus Software from time to time as per recommendations of the Antivirus Software provider.

ii. Maintaining up-to-date patch-states of the OS, browser, E-Mail, other software programs

iii. Maintaining back up of all valuable data stored in the Computer System in other storage media including external data media.

iv. Implementing best practices security e.g. password strength, regular changes of passwords, use of two-factor-authentication as recommended by Internet Service Provider, Social Media Service Provider, Financial Service Provider/Bank/Payment System Operator and/or Government/Authorities

*Note: Waiver of conditions (i) to (iv) above may be considered by the Company at its discretion, in cases of hardship where it is proved to the satisfaction of the Company that under the circumstances in which the Insured was placed, it was not possible for the Insured to take reasonable measures to safeguard the Insured's Computer System and Digital Devices and prevent the occurrence and to minimize the impact of any Cybercrime

H. CLAIM REPORTING/ PROCESS:

On happening of any loss or damage the insured or Upon receipt of any Claim, the Insured shall, as soon as practicable, give notice in writing/e-mail from registered email id with insurer thereof to the Insurer within 7 days but in any event not later than 14 days after the end of the Period of Insurance or Discovery Period, if applicable; and

if, during the Period of Insurance, the Insured becomes aware of any fact, event or circumstance which is likely to give rise to a Claim then the Insured shall give written notice thereof to the Insurer as soon as reasonably practicable and, in any event, during the Period of Insurance.

If the Insured reports a Claim or facts that might give rise to a Claim to the Insurer, then the Insured shall give the Insurer such information and co-operation as it may reasonably require including but not limited to:

a) Submission of fully completed and signed Claim form
b) Copy of FIR/Complaint lodged with Police Authorities / cyber cell
c) Copies of legal notice received from any Person/entity
d) Copies of summons received from any court in respect of a suit filed by a party/entity
e) Copies of correspondence with financial institutions with regard to any Loss
f) Legal notice served on any Financial Institution and or case filed against Financial Institution for IT Theft Loss
g) Copies of legal notice served on any Third Party for any Data breach or privacy breach
h) Copies of criminal case filed against third party

i) Copies of invoices for expenses covered under the policy for which indemnity is sought
j) Proof to show that the Personal Data is the propriety information belonging to the Insured.
k) Proof to show that Loss is incurred by the Insured.
Particulars of other applicable insurance, if any

All notifications and all communications under this Policy must be in writing to the address mentioned in the Schedule

I. DEFENCE SETTLEMENT AND CLAIM COOPERATION:

Insurer shall be entitled to fully participate in the defence and at the negotiation stage of any settlement that is reasonably likely to involve or appear to involve. However, the right and duty to defend and contest the claim shall lie solely on the Insured. As condition precedent to liability under the policy, the Insured shall provide the Insurer at his own cost with all documentation, information, assistance, co-operation that may be requested and required towards, investigation, defence, settlement or appeal of a claim or circumstances. Insured shall take all reasonable steps to mitigate the loss in his capacity immediately within reasonable period of time.

J. GRIEVANCE REDRESSAL MECHANISM:

If you are dissatisfied with any service, please contact the Branch Manager / Regional Manager of the local office which has issued the policy. If the issues are not resolved to your satisfaction by the local office, please e-mail or write to: customercare@---- or address--------. If you are still not satisfied, you can approach the Insurance Ombudsman in the respective area for resolving the issue. The contact details of the Ombudsman offices are mentioned below.