Cyber Insurance – A Risk Mitigation Tool for Cyber Risk in India

R. Raghavan *

The disruptions in cyberspace, can emanate from both natural events as well as through human accidental and intentional interventions. These man-made cyberspace disruptions are more onerous, and are occurring with increasingly alarming frequency, intensity and viciousness.

The 'e-space' ecosystem in India has undergone humongous transformation during the last few decades. This paradigm shift demands that platforms on which these are built are tamper-proof, and the user-edifices that control them, should be citizen-friendly, user-transparent and free of all types of vulnerabilities, any of which, if overlooked or mutualized, will portend enormous credibility crises having, financial social and ethical consequences particularly in a democracy.

This paper is an attempt to trace the vulnerability of India and her citizens to cyber-crime, explore the potential effects, and examine whether the risk of cyber-crime can be managed reasonably, with the insurance as an effective Risk Transfer Medium, inter alia, with various Public-Private Partnership measures to combat this ever-present threat.

Key words: Cyber Risk, Cyber Insurance, Cyber Liability, Reputational Risks, Cyber Risk Management

Introduction

Technology is already at the threshold of becoming the indispensable 'element' for survival like air, water and food, and a necessary resource for sustenance. Technology is both omnipresent, omnipotent and omniscient and also a threat, if misused. The dependence on technology will affect every citizen, rich and poor, urban and rural, literate and illiterate. The more the degree of dependence, even a moderate vulnerability will derail the institutional and individual continuance of activities crucial for the purported digitization revolution.

**Chief Operating Officer - ITI Re Ltd. E-mail: r.raghavan@itigroup.co.in*

** This paper was circulated as reading material in the NIA-FAIR Seminar on Cyber Risk, Liability & Management, November 23-24, 2017, Mumbai.*

The disruptions in cyberspace, as it obtains in the realm of catastrophes, can emanate from both natural events like flood, fire, etc., as well as through human accidental and intentional interventions. Whilst the former is typically misnomered as "Acts of God', the latter are the ones that defy the rules of the game and have to be endured almost with an attitude of fatalism. Whilst the Almighty has apparently no 'evil motive' to inflict such calamities, humans are inclined to be motivated by a variety of malicious intentions, and, therefore, their actions are more complicated and unpredictable and yet more difficult to fathom. Therefore, these man-made cyberspace disruptions are more onerous, and are occurring with increasingly alarming frequency, intensity and viciousness. Whilst on the one hand, the phenomenon is global, with no nation or community being immune to such vandalism, the after-effects can be disproportionately disabling for an emerging nation like India.

This paper is an attempt to trace the vulnerability of India and her citizens to cybercrime, explore the potential effects, and examine whether the risk of cybercrime can be managed reasonably, with the insurance as an effective Risk Transfer Medium, *inter alia,* with various Public-Private Partnership measures to combat this ever-present threat.

The Indian 'e-space' Ecosystem

The 'e-space' ecosystem in India has undergone humongous transformation during the last few decades. Several facilitating factors both within the country and those global in nature have contributed to this. To list a few:

- The Electronics Policy and the enabling infrastructure that have been put in place by the Government of India, right from the late 90's.
- The burgeoning IT industry supported by Global Service Providers from India, e.g., Infosys, TCS, and others.
- The aggressive pursuit of e-Governance by both the Central and State Governments
- The Mobile revolution making India as the World's second largest Subscriber base
- The large user-base for social media, like Facebook, What's App, etc., among the Indian masses, literate or otherwise.
- The recent full throttled "Digitization" drive of the Government of India, accelerating the ushering in of a "Cashless Society"
- The mushrooming of Start-ups and exponential growth, particularly in e-Commerce ventures.

- The huge number of IT/electronics professionals graduating, year-after-year managed by profit-motivated private engineering colleges, resulting in arbitrage of cost for BPOs, etc.
- The increasing interest in investing in Indian IT infra projects by global majors such as Amazon, Google, etc.

With almost 900 million Indians already enrolled for Aadhar as 'Proof of ID', it is invariably becoming a "surrogate DNA". This paradigm shift demands that platforms on which these are built are tamper-proof, and the user-edifices that control them, should be citizen-friendly, user-transparent and free of all types of vulnerabilities, any of which, if overlooked or misutilized, will portend enormous credibility crises having, financial social and ethical consequences, particularly in a democracy.

All the above developments are now snowballing into a collective digitised nation that will be the future India. It is an irreversible process that will make individuals and institutions inevitably flow with the momentum affecting their daily existence once the phase of adoption of technology has been successfully accomplished, because technology is acting as a catalyst and facilitating the development at a very rapid pace.

Definition of Cyber Risk

Given the complexity inbuilt into the cyberspace, any phenomenon associated with same also warrants a befitting resolution.

With the rapid evolution of the Information and Communication Technology (ICT), the cyberspace has morphed into a gargantuan risk, having three characteristics*: Invasiveness, Invisibility, and Interconnectivity.*

Since virtually all trade, finance and governance transactions overtly depend on IT, these three "I"s permeate all such services. Add to this all other forms of modern-day requirements, like transportation, services, healthcare, civic administration, education; all of this are without exception driven by ICT systems. Hence, the resultant impact of any disruption to or invasion of the ICT system/s supporting these functions would inevitably impact them adversely and have cascading ramifications.

Whilst the cyber laws in various national systems may have country-specific definitions, we can rather look at the underlying causes, intentions and resulting effects to understand the term "Cyber Risk" better.

The following definition, used in an exhaustive research paper of the Geneva Association, a think

tank founded by world's leading Insurance and Reinsurance community, seems to be the most apt for Cyber Risk:

Any risk emerging from the use of information and communication technology (ICT) that compromises the confidentiality, availability or integrity of data or services. The impairment of operational technology (OT) eventually leads to business disruption (critical), infrastructure breakdown, and physical damage to humans and property.

Cyber risk is either caused naturally or is man-made, where the latter can emerge from human failure, cyber criminality (e. g. extortion, fraud), cyber war, and cyber terrorism. It is characterised by interdependencies, potential extreme events, high uncertainty with respect to data and modeling approach and risk of change.[1]

The above definition appears to be a comprehensive one, in the sense, that it addresses the cause/origin of the risk, the manner in which the risk manifests, and the intentions/motives of man-made risk perpetrators.

To that extent, it makes it easy for any student analyst of Cyber Risk as it has clarity on the multi-dimensions of cyber risk.

Let us now look at the illustrations of the various components constituting the above definition, from events reported in the past to see how the various elements fit in.

Compromise of Confidentiality, Availability or Integrity of data or services

- There are enough instances of occurrences of this nature, ranging from the Data breach in Yahoo which aborted the $4.8 billion takeover move of the firm by Verizon- to the most infamous hacking of the dating site "the Ashley Madison' resulting in acute embarrassment and mental agony to hundreds of married couples.

  Edward Snowdown led "Wiki leaks" which made public, sensitive national security information.

- The Cyber heist of $ 81 million from the Central Bank of Bangladesh, in 2016 yet remains unresolved.

- The "Stuxnet" virus disabled the nuclear power plants of Iran.

- The alleged role of Russian hackers interfering in American elections is still 'headlines' in papers and a matter of contention between the Americans and the Russians.

[1] Ten Key Questions on Cyber Risk and Cyber Risk Insurance, The Geneva Association, November 2016

- The targeted attack on Sony Pictures in 2014, wherein the hacker group threatened and also carried out the threat of releasing unreleased films produced by Sony Pictures apart from leaking the database of Employee details and other particulars, including passwords.
- A St. Petersburg-based professional hacking company, named "RBN" can be hired at a price for any criminal hacking plot.
- In December 2012 Wells Fargo website experienced a denial of service attack, potentially compromising 70 million customers and 8.5 million active viewers. Other banks reported to be compromised are: Bank of America, J. P. Morgan US Bank, and PNC Financial Services.
- More revealing and scary are the findings of a study commissioned by Lloyds of London in collaboration with a Cyber Security think tank organization named "Cyence."[2]
- Excerpts from the Report:

  The recent "Wannacry " Ransomware attack, leading to not only sizeable bitcoin outflow but also non-availability of crucial health service data base in NHS of the UK.

  The direct economic impacts of cyber events lead to a wide range of potential economic losses. For the cloud service disruption scenario in the report, these losses range from US$ 4.6 billion for a large event to US$ 53.1 billion for an extreme event; in the mass software vulnerability scenario, the losses range from US$ 9.7 billion for a large event to US$ 28.7 billion for an extreme event.

  Economic losses could be either much lower or higher than the average in the scenarios because of the uncertainty around cyber aggregation. For example, while average losses in the cloud service disruption scenario are US$ 53 billion for an extreme event, they could be as high as US$ 121.4 billion or as low as US$ 15.6 billion, depending on factors such as the different organisations involved and how long the cloud-service disruption lasts for.

  Cyber-attacks have the potential to trigger billions of dollars of insured losses. For example, in the cloud services scenario insured losses range from US$ 620 million for a large loss to US$ 8.1 billion for an extreme loss. For the mass software vulnerability scenario, the insured losses range from US$ 762 million (large loss) to US$ 2.1 billion (extreme loss).

  These scenarios show there is an insurance gap of between US$ 4 billion (large loss) and US$ 45 billion (extreme loss) in terms of the cloud services scenario.

[2] Counting the Costs – Cyber Exposure Decoded, Emerging Risks Report, - Technology, Lloyds, 2017.

Meaning that between 13% and 17% of the losses are covered, respectively. The underinsurance gap is between US$ 8.9 billion (large loss) and US$ 26.6 billion (extreme loss) for the mass vulnerability scenario – meaning that just 7% of economic losses are covered.

When assessing current estimated market premiums against the forecasted cyber scenario insurance loss estimates set out in the report, it is apparent that a single cyber event has the potential to increase industry loss ratios by 19% and 250% for large and extreme loss events, respectively. This illustrates the catastrophe potential of the cyber-risk class.

These figures represent the mean values of simulated loss severities for large and extreme loss events, and take into account all expected direct expenses related to the events. Impacts such as property damage, bodily injury, as well as indirect losses such as the loss of customers and reputational damage are not taken into account.

These are illustrated as 95% confidence ranges – the range of values that act as good estimates to cover known and unknown parameters.

The Report draws the following Conclusions:

As the cyber threat increases, so too does the demand for cyber insurance.

- Despite this growth, the insurers' understanding of cyber liability and risk aggregation is an evolving process as their experience of cyber-attacks increases. It is therefore important that risk understanding, including technical premium calculations and capital models, keeps pace with the changing cyber risk knowledge base.
- In some other insurance cases, the insurers' understanding of liability and risk aggregation is more developed. It is widely accepted, for example, that natural catastrophies can trigger multiple claims from multiple policyholders, dramatically increasing the insurers' claims costs. Natural catastrophe insurance policies usually take this into account and reinsurance is commonly used to reduce the impact of risk aggregation.

The report's findings suggest that the economic losses from cyber-attack events have the potential to be as large as those caused by furious hurricanes. Insurers could benefit from considering the cover for cyber-attacks in these terms and make explicit allowance for aggregating cyber-related catastrophies. To achieve this, data collection and quality is important, especially because the modes of cyber risks are constantly changing and becoming more sophisticated.

Scope for Cyber Risk Occurrence in India

When endeavouring to get a feel of the scope for cyber risk incidence in India, one has also to take into account the magnitude and dimensions of the digital space in India.

Let us collate some numbers to map out the size and complexity:

The excerpts below are reproduced from the recent publication of the IT Industry's spokesbody NASSCOM:

The Report titled, "*Strategic Review 2017: India's Digital Journey"*, starts off with a major revelation:

> *"Digital technologies have been stamping their mark everywhere – these technologies are now on their way to being ubiquitous and are completing altering the way we do things – be it in the manufacturing process, business transactions, our interactions with our customers, suppliers, family, friends or government, etc."*

This being true geographically, it is all the more relevant to India. When we run through the listing of the developments in "Digital India", we are awestruck. Some pointers from NASSCOM:[3]

- Share of digital in IT-BPM exports has grown 4X over 2014-16, with leading players reporting a 10-15% share of their revenue from digital.
- Cloud and analytics accounted for nearly 3/5th of digital opportunities; from mobility and social account, an additional 15%; other areas of interest include: automation, IoT, robotics and AI.
- Significant enterprise focus has been on digitising mid- and back-office functions.
- Providers developing differentiated capabilities by re-skilling, setting up experience centres, labs and COEs in select areas of specialisation.
- Providers leveraging their clients, external partners and other ecosystem networks to identify/develop joint-solutions, acquisitions to deepen capabilities.
- Upcoming transition to GST, smart-city initiatives and industry-specific developments, offer several avenues of opportunity for IT-BPM players focusing on the domestic market.

Digital India - India's Journey to becoming a Digital Nation

- Initiatives include an ever-growing internet economy with increasing number of Wi-FI hotspots being enabled.
- Cashless, Paperless India – increased adoption of mobile wallets, Jan Dhan accounts, Aadhar,

[3] Nasscom Annual Report 2016

etc.

- Digital Literacy – skills training through NDLM and establishing Common Service Centres (CSCs).
- App Economy – Indians spent more than 140 billion hours on Android apps – the highest in the world (excluding China); India is to harvest the highest 5-year CAGR in app revenues.
- Citizen Services – Electronic delivery of citizen services through e-Kranti; 44 Mission Mode Projects (MMP) of which 25+ are operational; 222+ e-services implemented
- Goods & Services Tax Network (GSTN) – aims to provide a robust IT backbone for GST implementation.
- Smart Cities – Development of 60 Smart Cities during the FYs 2015-17; disruption and its continued impact was felt in 2016 in even greater measure, brought about by the usual suspects – IoT, Cloud, AI, etc.

Cyber Risk also poses a huge threat to the democratic and social process itself in the Indian context.

The intensity of digitization happening in India, due to the "Mission Mode" approach of the Government of India, can be gauged from their latest initiative: Launch of **"Crime and Criminal Tracking Network and Systems (CCTNS)** – whereby all the 15,398 Police Stations in the country would be connected enabling instant verifications of antecedents of any citizen under suspicion or scrutiny.

According to Mr. D. J. Patil, former Chief Data Officer of the US Government, India needs to be very concerned about cyber security and fake news as the country heads for the next general elections.[4] He goes on to say that there is going to be a massive shift in cyber-attacks which would increasingly be based on Artificial Intelligence.

Reported or Known Losses/ Incidents in India

Given the enormous spread and depth of the Information and Communication Technology (ICT) obtaining in India, no wonder that there is a substantial scope for vulnerability to cyber risks. There are several instances of media publishing cyber-attacks happening in the country.

Some of them are explicitly malicious attacks like 'defacing of websites or denial of access" suffered predominantly by government's Websites, usually suspected to be the handiwork of enemy nations like Pakistan. Other brazen events have been ATMs skimmed for bank cards and unauthorized withdrawals from unsuspecting customers' accounts. One of the nationalized banks was the victim of a debit card fraud running into several crores in 2017. There was also the recent

[4] Interview with D. J. Patil (former U.S. chief data scientist), The Hindu, July 25, 2017.

case of the Unified Payments Interface (UPI) administered by the National Payments Corporation of India that suffered an attack whereby Bank of Maharashtra, an associate Bank of UPI, reportedly suffered a financial loss of around Rs. 25 crores. The vulnerability was traced to a bug in the UPI solution procured by the bank, which was exploited by the hackers. Very recently, the e-Commerce Restaurant aggregator site, "Zomato" that admitted the compromise of a customer's personal details owing to a hacking incident.

Such incidents, perhaps prompted a key official of the Reserve Bank of India, to make the comment in January 2017.

S. S. Mundra, Deputy Governor of RBI had warned that banks need to have a robust defense mechanism against cyber incidents at all times.

He had said, "...our observation, however, is that many a times, certain finer details such as configuration of devices, patch management, OEM supported software, password management or port management, are ignored or entirely left to the vendors resulting in an undesirable impact. Statistics suggest that it takes on an average about six months to detect cyber-attacks by outsiders and longer in cases where attacks are by insiders. Thus, early detection and response assumes significant importance. Banks need to build capabilities to detect cyber-attacks early and respond to them quickly. Recovery from the incident is another aspect that needs to be well thought out."[5]

Adding to the agony, as is the wont, cyber risks materializing into incidents, carry an inherent "Reputational Issue" and, therefore, always tend to get either under reported or not reported at all. This is true, particularly of Institutions in the financial services sector as any adverse publicity of the vulnerability of such institutions results in an enormous dent on their credibility amongst their customers, leading to customer exiting in large numbers. This is not peculiar only to India but a globally common phenomenon. At least in developed markets, these institutions which deal with private personal and financial data and information, willy nilly carry some kind of insurance, which enforces compulsory reporting of such incidents to the authorities. But in India, the lack of the Insurance penetration, even against "Acts of God", leaves the reporting compulsion even superfluous. We therefore resort to the most credible source of data on such incidents, as available with "**CERT–In",** the Indian Computer Emergency Response Team, set up under the Ministry of communications and Information Technology, Government of India by an Act of Parliament.

The Information Technology Act, 2000, designated **CERT-In,** is designed and entrusted to serve as the national agency to perform the following functions in the area of cyber security:

- Collection, analysis and dissemination of information on cyber incidents
- Forecast and send out alerts of cyber security incidents

[5] Speech at Seminar on Financial Crimes Management arranged by CAFRAL, Mumbai on January 30, 2017

- Emergency measures for handling cyber security incidents
- Coordination of cyber-attack incidents and response activities
- Issue guidelines, advisories, vulnerability notes and whitepapers relating to information security practices, procedures, prevention, response and reporting of cyber incidents
- Such other functions relating to cyber security as may be prescribed

Cert-In is a member of several International Collaborative agencies for Cyber Security and is the last stop for any nation-wide counter action against cyber security threats.

The magnitude of cyber risk prevailing in India can be gauged from the following data furnished by Cert-In in their last Annual Report - 2015.[6]

Security Incidents Handled – 49455	Security Alerts Issued – 16
Advisories Published – 70	Vulnerability Notes Published – 316
Training Programmes Organized – 25	Indian Website Defacements Tracked – 26244
Open Proxy Servers Tracked – 1698	Bot Infected Systems tracked – 9163288

Out of the above-reported security incidents numbering 49,455, website defacements account for more than 50%.

Virus/Malicious codes figure as the next largest category, accounting for almost 20%. The other types of incidents are categorized as phishing, network scanning/probing, website intrusion and malware propagation, etc.

In the reply to a question in the Indian Parliament, during the latest Monsoon session in August 2017, the Minister of State for Electronics and Technology, Mr. P. P. Chaudahary replied that India was hit by 34 cases of ransomware on account of WannaCry and Petya attacks.[7]

A recent publication by Ernst & Young,[8] on the state of cyber-crime in India quotes a Mcafee estimation that around 0.21% of GDP is lost in India due to cyber-crimes, every year. The said report also goes on to illustrate several events, ranging from attacks of ransomware to phishing. According to a recent survey carried out by the firm, almost 26% of the affected entities belong to IT, Technology and Media segments and an equal proportion of the victims are from the Financial Services.

This has prompted the government to allocate Rs. 400 crores for setting up an exclusive Computer Emergency Response Team exclusively for financial services security against cyber-

[6] CERT-In Annual Report, 2015
[7] As reported in *The Hindu,* July 20, 2017.
[8] Responding to Cyber Crime Incidents in India, A Report by Fraud Investigation & Dispute Services, E& Y India, 2017.

attacks. The recent "Wanna Cry" ransomware episode, even though it did not result in any reporting of incidents in India, must accelerate efforts for preventive action.

As this paper is being written, there has been a massive cyber-attack across Europe, Ukraine and Russia. Ukraine Power Utilities have been disabled. Rosneft, the Russian Oil Major, had to shut down its main systems and switch over to its stand-by system. The computer systems of the shipping major, Meaersk were totally disrupted ny Non peta Virus, again an encryption attack demanding ransom payment in Bitcoins.

According to a cyber security firm's estimation, India was the worst affected amongst APAC nations.[9]

As recently as in early July 2017, two major incidents were reported in the media: India's largest Mobile service provider, Bharti Airtel, had a major outage at its New Delhi circle.

An event of greater concern is the reported hacking of Reliance Jio customer data base, and posting of details on a website.

The full scale of such breaches is yet to be divulged by both providers – for obvious reasons.

In fact, in a reply to a question in the Parliament, the Government of India admitted to a "Data Leak" leading to sensitive information about bank account details of beneficiaries, This is very weird as it involved several Government Departments.[10]

Cyber Risk Management: The Indian Framework

Against the background of the previous sections, India faces a multi-dimensional challenge with respect to cyber security. An expanding canvas of digitization pervading all aspects of public and private space, rapidly evolving changes in technology, cross-border collaboration amongst many segments of the economy, particularly in core areas like financial services, ICT, defence, and pharmaceuticals, on one hand, and, increasing competencies and collaboration among high value targeting by the hackers themselves on the other, present a scary scenario. Thus there arises the need for an overarching framework for constant alertness and proactive preparedness and crisis management against cyber-crimes. An endeavour of this expanse and criticality can expectedly be undertaken only by the government, at least in the Policy making stage and later to be complemented and contributed by private sector resources. All the more because the need for a robust cyber security is almost as paramount as the physical security of the nation. Any chink in this armour can be more deleterious and devastating than even an act of foreign aggression.

[9] The Hindu, July 11, 2017
[10] The Hindu, July 26, 2017

Let us therefore examine the political, legal and administrative framework for cyber security assurance within India. The Government of India has laid down the broad framework of cyber security aspirations in the "**National Cyber Security Policy, 2013".**[11]

As per the stated policy, the Vision, and Mission of the "National Cyber Security Policy, 2013, are as given below.

***Vision*: To build a secure and resilient cyberspace for citizens, businesses and government**

***Mission*: To protect information and information infrastructure in cyberspace, build capabilities to prevent and respond to cyber threats through a combination of institutional structures, people, processes, technology and cooperation.**

The policy then goes on to articulate the Objectives and Strategies to fulfill the Vision and Mission.

In effect, the Policy provides insight into the government's determination to: (a) create the necessary legal framework, infrastructure and the institutions for various preventive measures and crisis management functions; (b) seek collaboration across the borders as well with the private entrepreneurship within the country (c) lay down the base for the creation of CERT-In, and a National Critical Information Infrastructure Protection Centre.

As regards the legal framework is concerned, the IT Act, 2000, is the base legal framework (which has undergone amendments several times) under which the cyber security-related issues are identified and penalties listed.

The IT Act also addresses the important issues of security that are so critical to the success of electronic transactions. The Act has also given a legal definition to the concept of secure digital signatures. These would be required to be passed through a system of a security procedure, as stipulated by the government at a later date. Eventually, the secure digital signatures shall play a major role in the New Economy, particularly from the perspective of the corporate sector, as it will enable more secure transactions on-line.[12]

Under the IT Act, 2000, it shall now be possible for corporates to have a statutory remedy in case of an attack is perpetrated on computer systems or network and causes damages or copies data. The remedy provided by the Act is in the form of monetary damages not exceeding Rs.1 crore. This penalty of damages applies to any person who, without permission of the owner or any other person who is in charge of a computer, or computer system or a computer network, and:

[11] National Security Policy
[12] Cyberlwasindia.net

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

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/retrieval 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 database 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;

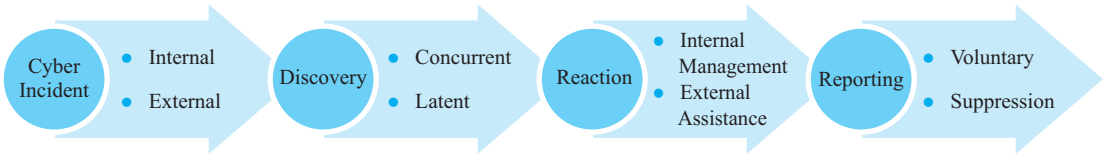
f) denies or causes the denial of access to any person authorised to access any computer, computer system or computer network by any means;

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 there under;

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.

The IT Act has defined various cyber-crimes, including hacking and damage to computer source, and, has declared them as penal offences punishable with imprisonment and fine. The various Amendments to the IT Act go beyond these provisions and also make it punishable to use the social media for various abusive purposes.

However, the cyber risk management in India has been following a very haphazard pattern.



In the above illustration, whilst incidents have been happening, CERT-In has been getting involved, but what is unclear is the non-availability of an organized framework for cyber risk management within the country. Depending upon which type of organization is affected, the management pattern may also vary from extreme confidentiality to one of mandatory disclosure. Even internationally, it has been observed that cyber risk tends to be viewed as a stand-alone risk area and not as an integral part of overall Strategic Risk Management.[13] Hence, in the Indian

context, it is even more unstructured. As for reporting, as there is no statutory requirement imposed by the cyber law in the country. The only compulsion appears to be the obligation to report significant events with financial implications to the Stock Exchanges, in the case of listed companies. The other categories like medium and small enterprises and quasi-government organizations are totally invisible in the cyber risk management horizon in spite of their higher vulnerability, and, therefore, higher potential for financial loss. This, as we will see later, will have an implication for cyber risk insurance.

Role of Cyber Insurance

What is the relevance of Insurance in the management of cyber risk?

Insurance has been a time-tested risk-transfer mechanism in the management of risks associated with property, financial stability relating to individuals, and organizations. Insurance comes to the succor, when either an individual or organization cannot afford to bear losses due to various causes beyond their control. As a pooling mechanism, the losses of few are paid by affordable contributions from many in a pool of risks.

By the same logic, given the increasing frequency and perceived quantum of cyber-attacks, it makes sense to resort to insurance as an ameliorating device for management of cyber risks too. Hence insurers/reinsurers have recognized their role in addressing the cyber risk requirements for insurance products and have been providing solutions exclusively for this special category of business for over two decades. As an evolving line of business, it is beset with both opportunities and challenges. More of it later. Now let us have a closer view of cyber insurance *per se.*

In the realm of General Insurance, the three broad categories of various products offered are:

(i) Property, (ii) Casualty and (iii) Liability

Whilst most of the dedicated infrastructure, which support the IT services of both corporates and individuals, are capable of getting covered under normal property policies against the perils of fire, inundation, internal mechanical or electrical/electronic break downs, etc., the real crux of coverage against cyber-crime is a different cup of tea altogether.

In the case of victims of cyber-crimes, the loss is generally of a legal liability under various laws governing Privacy and Integrity of Data.

Apart from these, there could be also loss of revenue, as in the case of Internet Service Providers, e-Commerce sites and the like, on account of interruption in services and denial of access. In the case of banks and similar financial services organisations, it could result in financial losses due to

[13] Swiss Re

fraudulent methods of looting customers' money and hence the liability to indemnify the same.

Cyber insurance provides specialised protection that is often not included in general liability policies. The list below of "Insurable Losses", in Cyber Insurance Policies, is compiled from the Cyber Insurance market as a whole.

(a) Cloud Cover: As software and data move from physical office networks to the cloud, cloud cover can protect the data held in the cloud.

(b) Intellectual Property: Protecting against claims for intellectual property rights' infringement in all forms of content, including user generated items.

(c) Cyber Crime: Being a victim of a malicious act, including phishing scams, telephone hacking, identity theft and wire fraud.

(d) Business Interruption: Covering the loss of net profit as a result of an interruption to a business after a cyber-attack or network security breach.

(e) Regulatory Investigations: Covering the cost of investigations and fines from data protection regulators in the event of a confidential data breach.

(f) Data Loss: Costs associated with data forensics, recovery, restoration and reorganization following a security breach or data leak.

(g) Cyber Extortion: If a hacker is threatening to damage the site or network, cyber extortion cover can pay the ransom payment demanded.

(h) Virus Damage: If a virus destroys the system, virus damage insurance covers costs to rebuild the computer systems and restore the data.

(i) Identity Fraud: If a hacker has fraudulently used the identity to enter into an agreement, the identity fraud insurance covers the costs incurred.

(j) Specialist Services: If the data systems have been compromised, the expensive specialist services to assess and repair any damage may be requested.

(k) Crisis Communication: In the event of a data breach, maintaining one's reputation is paramount, hence the crisis communication cover provides the specialist PR.

(l) Legal Expenses: The legal expenses cover provides expenses and advice for a range of IT-related disputes with suppliers and employees.

From the above listing of various types of insurance cover for specific cyber-attacks, one can easily conclude that most of the conceivable risk materialization possibilities, are getting

addressed through the instrumentality of tailor-made insurance schemes.

Availability of Cyber Covers in India

The Indian market, has characteristically been influenced always by the trends of product innovation in the developed markets, particularly when the demand for such products arises.

Given the dominant role that Indian software majors play in providing IT /BPO services to the developed economies, it is expected that the Indian insurance market will come up with the desired cyber risk products and offer them to their clients.

But what is surprising is that only three general insurers offering cyber insurance products could be located, upon scanning the list of products approved by IRDAI for the four years commencing in 2012. This, if this data is factually correct, then gives an impression that despite the enormous potential for this type of insurance coverage, the Indian insurers have not taken a plunge into popularizing and distributing the much-needed insurance cover schemes.

(ICICI Lombard, the largest private sector insurer in the country, projects that the Cyber Insurance Market in India will reach the US $ 750 million mark by the year 2020[14])

Insurance, as stated earlier, works on the principle of "Losses of few paid for by contributions of many". Therefore, given the increasing number of cyber-attack events, and, given the increasing vulnerability of organizations, in a country like India, the role of cyber insurance is very significant and a financially attractive business.

With the increasing use of internet, rapid digitization drive, high mobile user-base, the challenges of containing the financial losses to individuals and enterprises can be pooled and managed by the insurance mechanism. Even though, the IT products/services have not reached a "commoditized" profile, like the two-wheelers/four-wheelers, the day is not for off when the centralized service providing institutions, whose activities and functions affect the lives of even the ordinary people, may be subject to unpredicted cyber-attacks, resulting in partial or complete destabilization of the service network, controlled by IT configuration.

The latest such centralized institution is GSTN, the Goods and Services Tax Network. With the "One Nation, One Tax" platform, centrally handling the entire GST process management of the nation as a whole, it presents a perfect target for a planned attack (Given its vital importance, mission and critical role, one would expect that the promoters/managers would have taken every possible precaution to ensure its water-tight security). "Touchwood, if this central edifice is hacked, it would result in denial of service, or data corruption or encryption, and if a fabulous ransom is demanded by the hackers, one can visualize the magnitude of economic woes and chaos, financial loss and credibility that the government would face and the consequent political

[14] Report of The Telegraph , issue dt.17/07/17.

and social repercussions to the entire nation. The entire trading network in India may collapse, will get disoriented and destabilized (It is not a remote or unlikely scenario, given the fact that even the FBI and the defense establishments in US, have been victims to this menace).

In terms of damage control, the compensatory financial outgo, of a promoter entity, which is essentially a Not-for-Profit Private Company, is expected to process 3 billion invoices a month, can suffer a huge loss. Such an event can also have a cascading effect on the trading community, either big or small, that transacts daily through this organization.

There are numerous such service providers, both public and private, national or international, located in India, who are vulnerable to cyber-attacks. The recent case of the Dutch-owned Maersk Shipping Line, which suffered a global cyber-attack due to Non peta virus ransomware, is a classic case of trans-border, impact – its Indian arm services in JNPT, also were also disrupted, forcing discontinuance of services for some days.

Thus, insurance can serve as a reliable financial risk-transfer solution.

Beyond this role, there are other ways, wherein insurers can play a constructive role:

- Insurers would not undertake or assume risks which they do not understand and re unable to quantify. This means they have to model the risk in terms of the probability of frequency and magnitude of such occurrences. Whilst, this being a very nascent line of business, there is a lot of ground to be covered in this area. Substantialfforts have already gone into providing certain reasonable profiling of cyber risk due to various contingencies and various type of organizations.
- Such estimations, apart from providing decision tools for insurers for their product design and pricing urposes, can incidentally assist the insured organizations to recognize their own risk profile and vulnerabilities, coming as it is from a larger canvass of insured organizations, thereby benefitting, from a wider insight.
- Insurers oppose 'nti-selection' Hence, they will undertake a re-acceptance inspection and assessmentof midsize and larger organizations from a risk prevention perspective. This would benefit the client organization and plug the loopholes lest they face higher premiums and restried coverage.
- Many Insurers/reinsurers have collaborative arrangements which, in case of events materializing, will come into play for large-scale disaster management efforts, spread across organsiations suffering from similar triggers or outbreaks, like ansom ware.
- B*y asking the right questions in addressing cyber risks, insurers and insurancerokers can*

help promote the adoption of good practice, including the Government' Cyber Essentials cheme, which will reduce the frequency and cost of breaches ccording toRt Hon Francis Maude, MP, Ministr for the Cabinet Office, UK.[15]

Hence, there is tremendous scope and potential for the Indian cyber insurance companies to play a catalytic and developmental role in the cyber risk management of our nation.

Opportunities and Challenges

Given the vibrancy of the Indian Non-Life Insurance Market, and also making use of the huge talent pool of IT resources available in India (Aadhaar is globally a unique success story), and if the right platform is evolved, cyber insurance can grow in geographic and geometric terms.

The financial exposure estimations done in the UK place the Global Cyber Exposure close to $160 bn with a Probable Maximum Loss, ranging between 0.15% and 20%, depending upon the type of events and the firm/s which are likely to be affected. Whilst these estimations could yet be largely redundant in the case of India, the potential for a few millions of dollars exposure cannot be ruled out.

As mentioned earlier, ICICI Lombard, the largest private insurer, estimates the potential income from Cyber Insurance premium to reach US$ 750 million by 2020[16]. Nevertheless, to attain a critical mass, there are several challenges, listed below, to be met:

1. The hard reality is that the awareness of the utility of cyber insurance as a risk mitigation tool is nearly absent except in large IT driven or IT solution providing firms and MNCs.
2. Practically no standardized and customer-friendly product has been made available in the market. There are various versions, leading to information asymmetry in this complicated and nascent domain yet to be sorted out.
3. Due to lack or loss of data, insurers, in almost all classes of business, rely upon past data of insurable events, on the basis of which they gauge their exposure and accordingly determine the pricing. It is anybody's guess whether any amount of credible data is at all available. The problem is magnified by the fact that, there is no mandatory reporting obligation for firms that have suffered cyber incidents nor is there any formal or informal pooling of information on such incidents even among the Insurance Community, leading to a tendency to follow the any of the reinsurance practices or adopt the London market pricing approaches.
4. There is a total disconnect currently between various agencies involved or required to be involved in cyber risk management within the country. For instance, in the entire IT Security Policy or the Cert-In scheme, there is a conspicuous absence of any reference whatsoever to Cyber Insurance. Compare this with the initiative that the UK Government has taken in 2015,

[15] HM Government, Report "UK Cyber Security: The Role of Insurance in Managing and Mitigating the Risk", March 2015.
[16] The Telegraph issue dt.17th July ,2017

by combining the Department of Trade and Industry and the Insurance Industry, leading to the publication of a report titled, UK Cyber Security: The Role of Insurance in Managing and Mitigating the Risk" in March 2015". This yeoman effort lays down the role of insurance industry in augmenting cyber security and aims to develop cyber risk expertise and export the same to other countries. The envisaged framework provides for information sharing as well as standardization in cyber security measures in the firms.

5. The approaches to bring about IT security measures again are fragmented – RBI, SEBI, IRDAI for example, have no coordination in their mandates even though, all these sectors have overlapping functional areas / interdependencies.

Recommendations

From the foregoing, it is evident that there are three major areas where substantial efforts have to be undertaken to promote insurance as a meaningful and effective risk-mitigation mechanism for preventing and controlling vulnerability and post-event financial and other type of losses of the firms. These are:

1. Creation of awareness of insurability of cyber risk.
2. Designing and distribution of user-friendly and reliable cyber insurance products.
3. Cohesive engagement of the agencies concerned, *viz*. the government, the insurance industry, and the IT-User/Provider community, with respect to coordinated *ex ante* prevention efforts, information sharing and synchronized *post-facto* disaster management.

Hence, it is felt appropriate to make the sector-wise recommendations as below:

The Government

In the monsoon session of the Indian Parliament in August 2017, in response to a specific question, whether the Government of India has planned to amend the existing regulations for promotion of cyber security, the Minister of State for Electronics and Technology replied in the negative saying: "Presently there is no proposal to amend the Information Technology Act, 2000". In a separate reply, the Minister added that the IT Act provided a legal framework to deal with cyber security breaches.[17]

While one cannot conclude that this attitude tantamount to complacency, expecting a legal framework to take care of cyber security would be wishful thinking, to say the least. Hence, it is recommended that the Govt.:

- Set up a Coordination Platform under the aegis of the Ministry of Information and Technology, CERT-In on a PPP model. Such an agency can aid in evolving state of the art

[17] As reported in The Hindu dt.20 th July, 2017

cyber security measures, evolve effective security standards to be adopted by various types of organizations like corporates, MSMEs, individuals, etc. The recently set up **National Critical Information Infrastructure Protection Centre** has also to be necessarily roped into this platform.

- Bring about legislated mandates on all providers/users to adopt such standards and get accreditation from quality certifying institutions.
- Set up a Data/Information pooling platform wherein all cyber events or near misses should be reported by law, suitably safeguarding privacy and reputational concerns.
- Provide incentivasion though measures like tax breaks for firms opting for accreditation.
- Ensure cooperation with developed nations to bring about coordinated intelligence and counter measures for combatting malicious cyber-crimes like politically motivated or criminally organized cross-border cyber-attacks.

The Insurers

- Under the Self-Regulatory Organization, viz. General Insurance Council, set up a Task Force for Cyber Insurance.
- The task force can induct specialists from the faculties of IT, IT Security, underwriters, reinsurers and consumer representatives.
- The role of the Task Force is to collect and collate data on cyber incidents, provide for information sharing between the insurance community, user-community and the government
- Lay down a target enrollment ratio of all corporates and MSMEs as well as other Not- for-Profit Institutions like universities to be achieved by defined timeline.
- Endeavour to determine loss scenarios and possibilities, securing assistance form international reinsurers and modeling organizations.
- Estimate the potential loss aggregations and calibrate the same against available domestic insurance capacity and reinsurance availability.
- Set up pool arrangements similar to “Terrorism Pool” and “Nuclear Pool”, and, if there is a sizeable supply gap, seek Government's Involvement as the “Insurer of last resort”.
- In competitive spirit encourage product innovation and differentiation among member insurers.
- Dovetail a disaster-response arrangement commonly available to all insuring firms in coordination with CERT-In.

- Ensure adequate dissemination of product availability and set up Points-of-sale.
- Have continuous dialogue with similar international agencies like the Association of British Insurers (ABI) to have contemporary state of knowledge on matters related to cyber Security.

The Regulator

- Treat cyber insurance as a separate class and not just part of a miscellaneous type of business
- Proactively engage insurers to launch cyber insurance products.
- Provide for suitable relief in the Solvency Margin calculations as also in the reinsurance restrictions.
- Help create and nurture a pool of domestic cyber capacity.
- Enable the simplification of the product from a Policy Holder Protection point of view and help standardization of terms and conditions as has been done in the case of health insurance.

The Customers

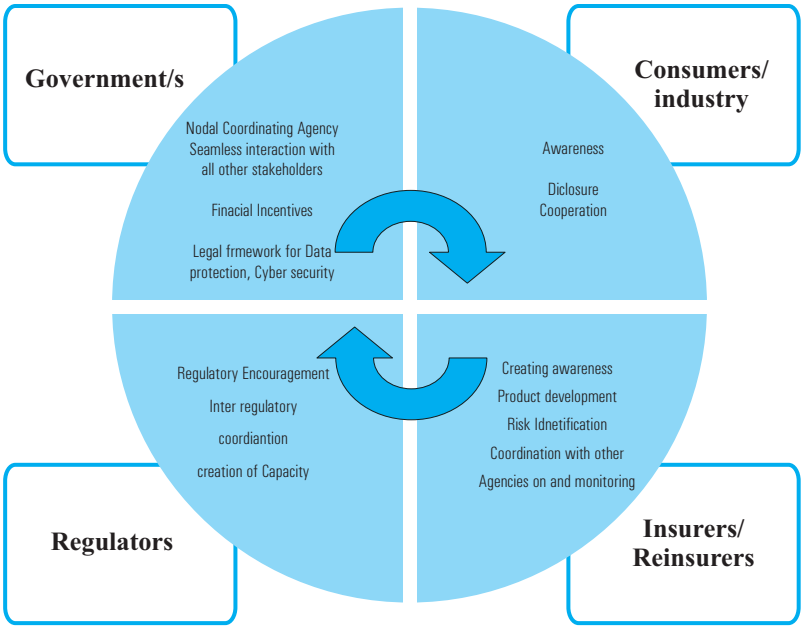
- Make cyber security as an integral part of the enterprise risk management and involve the board in the perception and direction of cyber risk management.
- Engage constructively with the accreditation agencies for obtaining the cyber security certification.
- Actively explore risk transfer through appropriate insurance purchase
- Have a continuous interaction with insurers to have an updated risk management practices.
- Share "Near Misses" and seek guidance from both insurers and security professionals.
- Bring about the need for cyber insurance in industries like NASSCOM, CII, FICCI, etc.
- Imbibe and internally disseminate the availability and utility of cyber insurance.

The Way Forward

Physical security is no doubt paramount and being so tangible, it is evidently addressed in all its aspects through various protective measures.

Whereas cyber insecurity is the 'Uncertain Factor" lurking around every corner,, unless an holistic approach is conceptualized, resourced and implemented on a continual basis, the whole nation would stand continuously exposed.

An illustrative construct of such an approach is presented below for the consideration of all the concerned players.



As was realized, albeit post facto, in the World Trade Centre attack, what is the most vital in any terror or similar covert or concerted attack against nations or societies is "joining the dots". From that perspective, it is highly desirable that all possible agencies come together for countering cyber risks – including Insurers in this War on Cyber Risks.

Summary

1. Cyber Security is ballooning into a cause of major concern for all organizations, governments and individuals world over.

2. The recurring frequency of Cyber-attack events added with increasing complexity juxtaposed with an ever increasing dependency on Information and Communication Technology(ICT) in all walks of life, is making management of Cyber risk increasingly onerous and inevitable.

3. Given the omnipresent nature of ICT, to manage" Cyber Risk" effectively, it is paramount have clarity of thought as to what we mean by the term "Cyber Risk".

4. In an emerging economy like India which is morphing into a "Digital Nation" , it is imperative to recognize the extent of vulnerability to Cyber Risks, the country faces.

5. It is very evident that India faces a serious level of vulnerability, which makes it abundantly apparent, that we cannot afford to gloss over Cyber Security concerns any more.

6. The incidents in the past and of very recent times ,of Cyber Risk Events in India , clearly attest to the potential threats and challenges in the country, due to Cyber Security issues.

7. In this context, it is essential to examine the extant framework for management of Cyber risks as present now in the country. This scrutiny , reveals that even though well intentioned, the Legal- Executive and User interface framework as it exists now, still carries quite a few blind spots.

8. Very glaringly, this framework does not even refer to Insurance as a Risk Transfer mechanism, even in the passing! This is in sharp contrast to the frameworks elsewhere in developed markets, wherein , either by statute or by voluntary collaboration, Insurance kicks in as an essential risk management tool.

9. In this hazy state of affairs, we have to recognize the constructive role insurance can play in Cyber Risk management, in not only mitigating the Cyber fallout through post facto financial loss indemnification but also as a proactive 'ex ante" prevention mechanism.

10. In this background, the attempt to decipher the awareness of and availability of Cyber Coverage in India leaves much to desire.

11. There are just three IRDAI approved products in the market.

12. Therefore, the business line of Cyber Insurance in India is bestowed with lot of growth opportunities but also is beset with concomitant challenges. The latter challenges are not entirely peculiar to India but nonetheless get exacerbated as compared to those facing Insurers in developed markets ,on account of the nascent stage of Cyber Security environment in the country.

13. In this back drop of the need to manage Cyber Risks effectively through use of Cyber Insurance,, it is recommended that those who shape the Cyber security Universe in the country and administer the management of same- the Government, the Regulators, the Industry and other members of the ICT community ,coordinate the efforts for ensuring national cyber security through proper interaction with and involvement of Insurers/reinsurers.

Such teaming up will:

a) raise the awareness of Cyber Vulnerabilities across the board

b) set standards for Cyber defense

c) provide a larger and credible Cyber Loss data base for all concerned to exploit for preemptive plan of action as well as post loss coordination

d) mitigate economic losses

e) ensure emergence of a " Safe and Secure Digital India"

References:

- https://www.ivw.unisg.ch/_/media/internet/content/dateien/instituteundcenters/ivw/studien/studie-10-key-questions.pdf
- https://www.lloyds.com/news-and-insight/press-centre/press-releases/2017/07/cyber-attack-report
- http://www.nasscom.in/sites/default/files/NASSCOM_Annual_Report_2016-17.pdf
- http://www.thehindu.com/news/cities/bangalore/ai-will-have-huge-impact-on-indian-jobs-former-us-chief-data-scientist-dj-patil/article19303589.ece
- https://www.rbi.org.in/Scripts/BS_ViewBulletin.aspx?Id=16722) (RBI Bulletin February 2017
- http://www.cert-in.org.in/
- http://www.thehindu.com/news/national/india-hit-by-34-ransomware-attacks-minister-tells-ls/article19309469.ece
- http://www.ey.com/Publication/vwLUAssets/ey-responding-to-cybercrime-incidents-in-india-new/$FILE/ey-responding-to-cybercrime-incidents-in-india.pdf
- http://www.thehindu.com/news/national/centre-admits-to-data-leak/ article19365883.ece
- http://meity.gov.in/content/national-cyber-security-policy-2013-1