DSCI
PROMOTING DATA PROTECTION
A NASSCOM® Initiative

CYBER INSURANCE IN INDIA

Mitigating risks amid changing regulations & uncertainties

DSCI
PROMOTING DATA PROTECTION
A NASSCOM® Initiative

About DSCI

Data Security Council of India (DSCI) is a premier industry body on data protection in India, setup by NASSCOM®, committed to making the cyberspace safe, secure and trusted by establishing best practices, standards and initiatives in cyber security and privacy. DSCI works together with the Government and their agencies, Law Enforcement Agencies, industry sectors including IT-BPM, BFSI, CII, Telecom, industry associations, data protection authorities and think tanks for public advocacy, thought leadership, capacity building and outreach initiatives.

Copyright & Disclaimer

RAMA VEDASHREE
CEO, DSCI

FOREWORD

Although 'VUCA – Volatility, Uncertainty, Complexity, and Ambiguity' as a notion was introduced around 1990s, the current age and time can very well be defined by it. The world is changing at a fast pace, thanks to digital technologies. While technology and the interconnectedness empower human beings, there are looming risks and uncertainties that accompany such technological proliferation. Our level of preparedness towards uncertainties is a key factor that determines success.

Undoubtedly, the awareness around cyber risks has increased in India, with more number of industries and verticals ensuring better security measures. However, attacks continue to get sophisticated, and regulatory environment is evolving around data and privacy, which necessitates having a better and holistic risk management strategy. This prompted us to explore 'Cyber Insurance' as a topic of discussion. Cyber Insurance helps mitigate risk exposure by offsetting costs after a breach and has a corollary benefit of improving the adoption of preventive measures. We have been receiving several queries on this topic, and we felt that it is extremely pertinent in the cyber security space to have awareness on cyber insurance, to be able to ask the right set of questions for better coverage and premiums.

Covering both market and technical insights globally and of India, DSCI's report 'Cyber Insurance in India - Mitigating risks amid changing regulations & uncertainties', is aimed at increasing awareness, initiating deep-dive discussions, and providing directional insights to various stakeholders – Buyers, Carriers/Insurance Providers, Technology Firms, Brokers, Govt./Regulatory Bodies and Associations, on how concerted efforts can improve cyber resilience of organizations. We hope you find the report informative, and we invite your feedback and comments at industry@dsci.in.

ACKNOWLEDGEMENT

ACKNOWLEDGEMENT

Our sincere thanks to the experts who provided their valuable insights for the study.

Marsh India Insurance Brokers Pvt. Ltd.
Bhishma Maheshwari, Cyber Leader
Ritesh Thosani, Cyber Team

Tata AIG General Insurance Company Limited
Najm W. Bilgrami, National Head, Financial Lines

FireEye Inc. – Mandiant
Shrikant Shitole, Senior Director & Country Head - India & SAARC at FireEye, Inc.
Vivek Chudgar, Senior Director, Mandiant Consulting (APAC)

DSCI TEAM

Vinayak Godse, Vice President
Manishree Bhattacharya, Manager – Research (Industry Development)
Amit Ghosh, Assistant Manager – Communications

EXECUTIVE SUMMARY

CYBER INSURANCE

Insurance products designed to mitigate risk exposure by offsetting costs, after a cyber-attack/breach.

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).

INDIAN CYBER INSURANCE OVERVIEW

01 **~350** cyber insurance policies sold till 2018, a 40% increase from overall base in 2017

02 India's yearly cyber premium in the range of **INR 80-100 Cr** (USD 11 to 14 Mn)

03 **IT/ITes and Banking & Financial Services** are early adopters

04 **Newer demands** from manufacturing, pharma, retail, hospitality, R&D and IP-based organisations

05 For 1 Mn USD coverage, premium amount ranges from **USD 6,500 – USD 8,000**

Based on Expert/Market Insights

EXPERT COMMENTS

Prominent data breach events in the U.S. and the Western world, and recently enacted laws such as the European Union's General Data Protection Regulation (GDPR) is driving the uptake of cyber insurance by Indian firms, with global exposure.

- ***Anup Dhingra, President – FINPRO & Private Equity M&A, Marsh***

Robert S. Mueller, III, Director FBI said and I quote "There are only two types of companies - those that have been hacked and those that will be hacked." The growing digitalisation of the economy will continue to create challenges in terms of managing digital security and privacy risk. I believe, Insurers shouldn't sell this as an insurance policy, but really work on providing a complete solution through pro-active forensic services and legal consultation at the time of claims. They should also offer 'after sales value added services' like cyber maturity audit to let the Insured know the weaknesses in their cyber security framework.

- ***Najm W. Bilgrami, National Head, Financial Lines at Tata AIG General Insurance Company Limited***

Many Indian firms are competing on the world stage, so they face considerable cyber risk from advanced threat actors. While there is no panacea, cyber insurance can help improve a firm's resilience following a breach. Technology firms can work hand-in-hand with insurance providers to develop innovative, industry-specific solutions, that can provide a better ROI for all stakeholders.

- ***Vivek Chudgar, Sr. Director - Mandiant Consulting (FireEye Inc.)***

TABLE OF CONTENTS

CYBER INSURANCE

The Global Perspective

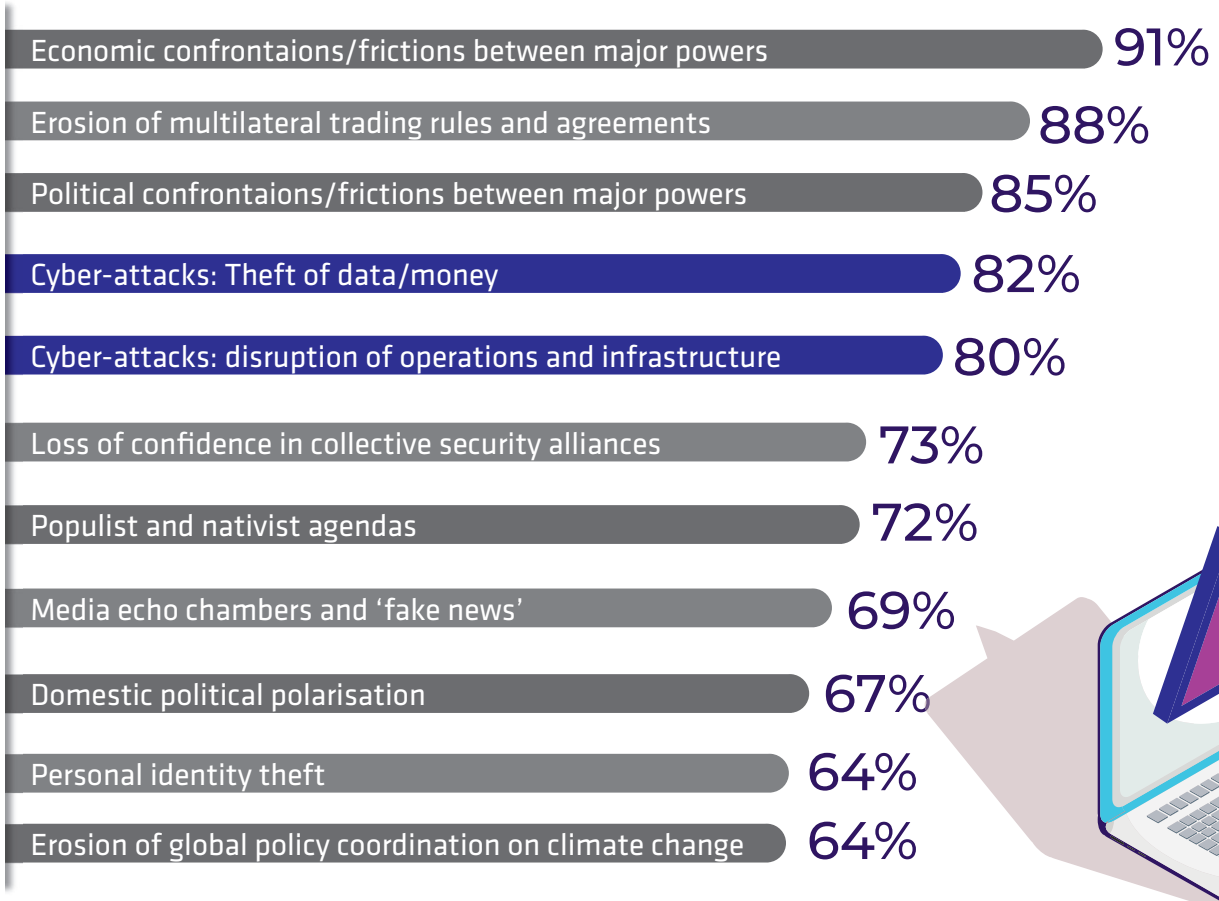
CYBER ATTACKS

Emerging as one of the top risks globally

In today's age and time, amid talks around climate, health and geo-political risks, cyber risks have also drawn significant attention. Whether it is an individual, corporate or Government, technology and digitisation have touched upon all entities. Digitisation continues to generate tonnes of DATA, which when used prudently can become an important and coveted asset. The world is also at a critical juncture, where geopolitical equations are redefining businesses and growth, and the vortex of different political ideologies and narratives are disseminating at a fast pace, with the help of technology. When these aspects are intertwined, attacks such as identity thefts, social engineering, cyber warfare, cyber terrorism, network lockdowns, and state-sponsored cyber espionage – all become a matter of reality today, making cyber risk even more pertinent, as it elevates attacks from an individual level to that of a 'State'.

WORLD ECONOMIC FORUM GLOBAL RISKS PERCEPTION SURVEY 2018–2019

Percentage of respondents expecting risks to increase in 2019



INSTANCES HIGHLIGHTING LARGE-SCALE CYBER ATTACKS

01 Atlanta smart city network lock down (2018)

02 Massive power outage in Ukraine, leading to blackouts (2015)

03 Sensitive health data of 1.5 Mn patients, including Prime Minister's, stolen in Singapore (2018)

04 The WannaCry ransomware cyber attack Worldwide – infected NHS, London and Telefonica, Spain, among others (2017)

05 IoT botnet Mirai attacked DNS firm Dyn that disrupted Twitter, Netflix, Reddit and a host of other major sites in the United States (2016)

Source: World Economic Forum-Marsh The Global Risks Report 2019; DSCI-PwC Report 'Creating Cyber Secure Smart Cities; Insurance Journal

IMPACT OF SECURITY BREACHES

Spanning monetary to reputation loss

53%

CISCO 2018 ANNUAL CYBER SECURITY REPORT

of all attacks resulted in financial damages of *>USD 500,000 (including, but not limited to, lost revenue, customers, opportunities, and out-of-pocket costs)*

Notpetya Malware Attack
A total of USD 10 Bn in expenses

WannaCry Ransomware Attack
USD 4 Bn in financial losses globally

Under **GDPR**, fines of upto EUR 20 Mn (~USD 22.75 Mn) or 4% of annual turnover

LOSES & PENALTIES

AVERAGE COST OF A BREACH (BY SECTOR)*

Most cyber claims filed by small businesses with revenues under USD 50 Mn

*Based on analysis of 1,201 claims by NetDiligence, for incidents that occurred between 2013-2017

Digitalisation of businesses (via Cloud, BYOD, Mobility, Social Media, and IoT) have increased threat surface and vulnerabilities. At the same time, attacks are becoming more complicated, menacing, and stealthy. To top it, the risk of insider threat makes it extremely difficult for an organisation to ensure a 360^0 safeguard from attacks.

Apart from the direct monetary loses, the hidden costs of a data breach, which includes lost businesses, partnerships, and reputation could be even more debilitating, necessitating a better risk management and cost-offsetting strategy.

Source: CISCO Annual Cybersecurity Report; Symantec Blog; Information Security Newspaper; IT Business Edge; NetDiligence

PUTTING SPOTLIGHT ON 'CYBER INSURANCE'

Mitigating risks amid uncertainties and changing landscape

WHAT IS CYBER INSURANCE?

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.

HOW CAN CYBER INSURANCE IMPROVE THE CYBER SECURITY POSTURE OF A COUNTRY?

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.

TYPICAL COVERAGE

Response to breach events

(notification, call center services, breach resolution, mitigation services, public relations, and crisis management)

Regulatory coverage

(Costs for notification, defense, penalties)

Liability coverage

(Privacy, security, multimedia liability)

Cyber extortion and deceptive fraud transfer

Institution's loss of income or extra expenses

(due to security breach including third parties, system failures, voluntary shutdown of systems following an attack)

Data replacement/recovery costs

Source: Expert Insights; Institute for Defense Analysis; CIO

KEY STAKEHOLDERS

An intermesh of internal and external stakeholders

KEY STAKEHOLDERS INVOLVED

The Insured (First Party)
Buyer of cyber insurance policies

Broker
A broker acts on behalf of the buyer – facilitates the buying process; helps understand and quantify risks; provides recommendations on insurance carriers or policies that might be favorable for the organisation; helps obtain appropriate coverage and favorable pricing

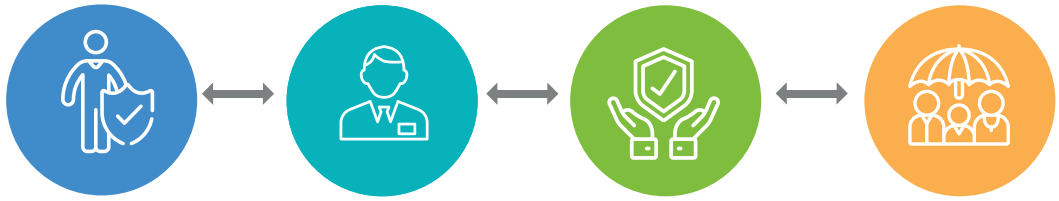
Carriers/Insurance Providers (Second Party):
A carrier is an insurance provider

Reinsurers
Another insurance company that takes care of the risks to the primary carrier

Cyber Security Product/Service Provider
A tech company that provides cyber risk assessment. Technology firms are also engaged to conduct forensics and/or incident response services post a breach

The government and regulatory bodies have an important role to play to enable the cyber insurance space in a country. For the Insured (insurance buyer), there are many internal stakeholders involved, which includes the CEO, Board, Third Party Vendors, Operations, Communications, Customers, CFO, Compliance, HR, Legal, IT and Risk Managers.

BUYING AN INSURANCE
A STEP-BY-STEP PROCESS



The Insured (insurance buyer)

- Reaches out to a broker to buy a policy cover
- Employs a tech provider (upon being advised by the broker) for cyber evaluation

Broker

Broker facilitates the buying process

- Helps understand and quantify risks
- Provides recommendations on insurance carriers
- Helps in reaching out to carriers to get quotations
- For better premium, suggests the buyer to engage with a tech provider for complete cyber evaluation and (if needed) fortification

Carriers (insurance provider)

- Sends out risk assessment questionnaire to the buyer
- Asks for details on Business Continuity measures
- Can engage with third party for cyber risk assessment of the buyer
- Finally, provides quotation

Reinsurers

- Another insurance company that takes care of the risks to the primary carrier

Cyber Security Product/Service Provider

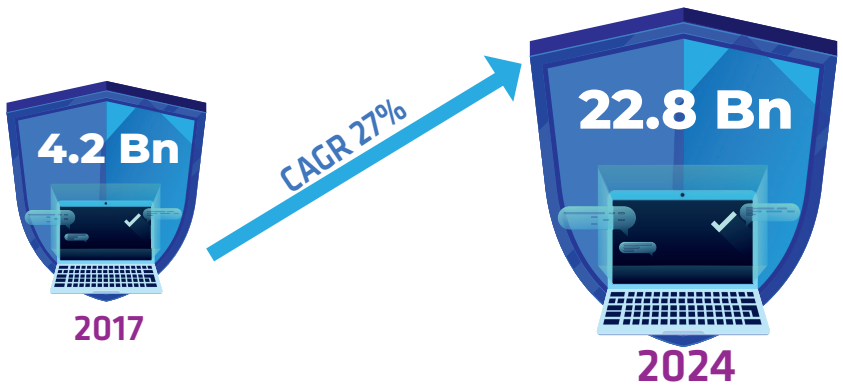
Can be engaged either by the buyer or the carrier

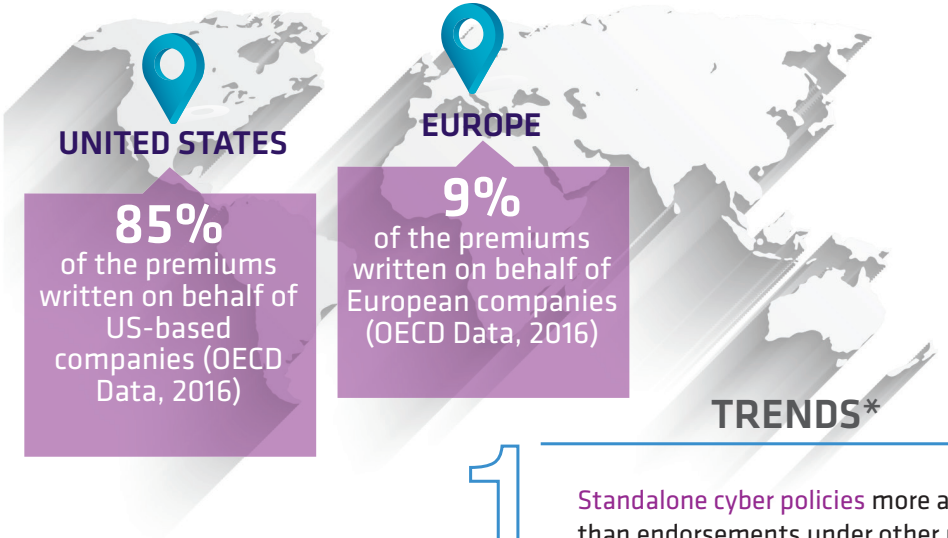
Source: Expert Insights

GLOBAL MARKET

Expected to grow at a CAGR of 27% from 2017 to 2024

CYBER INSURANCE GLOBAL MARKET





NOTEWORTHY PLAYERS

Allianz Global Corporate & Specialty
American International Group, Inc.
AON PLC
Beazley PLC
Berkshire Hathaway, Inc.
Chubb Corporation
Lockton Companies, Inc.
Munich Re Group
XL Group Ltd.
Zurich Insurance Co. Ltd.

KEY SECTORS

BFSI
IT/ITes & Telecom
Retail
Healthcare
Manufacturing
Professional Services

TOP DRIVERS

- News of cyber-related losses experienced by others, or experiencing loss themselves
- Third-party requirements (e.g. customers, partners)
- Increased education/awareness
- Demand from the Board or senior management
- Regulatory changes
- GDPR continues to be a concern

KEY CHALLENGES

Lack of understanding of

- Risk exposure
- Coverage options
- Pricing
- Application process

TRENDS*

1. Standalone cyber policies more attractive than endorsements under other policies
2. New coverages that renewal buyers are interested in – cyber related Business Intelligence, fund transfer frauds/social engineering, data breach, cyber extortion/ ransom
3. Majority of new-to-market buyers are small (revenues <50 Mn) and mid-size companies (revenues 50 Mn to 1 Bn)
4. Demand for expansive portfolio, pre and post breach support services, and risk assessment
5. Coverages continue to evolve to address new regulatory changes

* Trends are based on a survey of brokers and underwriters (primarily from the US) by PartnerRe & Advisen

Source: Zion Market Research; OECD Report; PartnerRe & Advisen Trends Report; Aon White Paper; Willis Towers Watson Wire Blog

GLOBAL INITIATIVES

Exploring insurance as a means to improve resilience

UNITED STATES

UNITED KINGDOM

RECENT REGULATORY DRIVERS

Security Breach Notification Legislation

EU General Data Protection Regulation (GDPR)

INITIATIVES OUTLINED

- The US department of Homeland Security worked towards creating a conducive environment where cyber insurance promotes adoption of preventive measures and best practices in return for better coverage and premiums
- Between 2012 and 2014, hosted several cybersecurity insurance working sessions, and identified 3 key ideas:
  - Cyber incident information sharing
  - Cyber incident consequence analytics
  - Incorporating cyber risk into Enterprise Risk Management (ERM)

- Develop guides on cyber insurance and host it on govt. website
- Government and carriers to collaborate for data pooling and exchange, that can further help in determining better premiums and coverage for more resilient firms. Utilize this data pooling forum to improve insights on risks and cyber disaster scenarios
- Firms encouraged to have better risk management framework, a recovery plan, and conduct stress testing to check financial resilience in various scenarios
- Helping London become a global centre for cyber risk management

For SMEs: Government's Cyber Essentials for SMEs to be used by carriers as part of their cyber risk assessment, which will encourage more SMEs to adopt Cyber Essentials.

Source: Aon Report; Department of Homeland Security Website; National Conference of State Legislatures; IT Governance; UK Cyber security - The role of insurance in managing and mitigating the risk

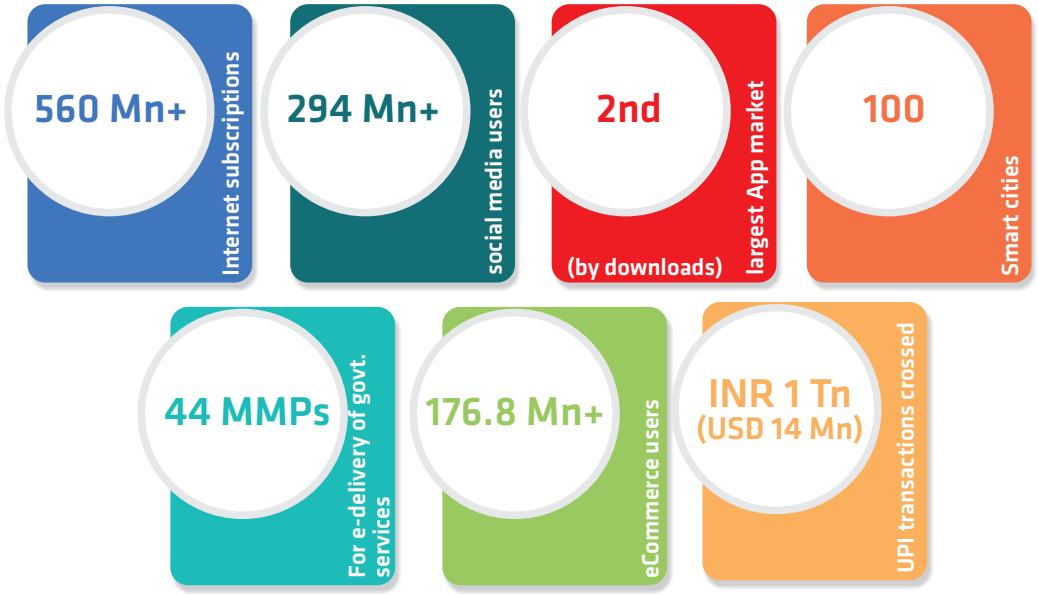
CYBER INSURANCE

The India Perspective

CYBER RISKS IN INDIA

Why is 'Cyber Risk' entering mainstream narrative?

BURGEONING DIGITIZATION



IT & IT-enabled services, eCommerce, Digital Payments, Cyber Security, Deeptech, Fintech, Healthtech, OTT & Mediatech

RISE IN SECURITY BREACHES

India **2nd most affected country** due to targeted attacks (for attacks between 2016 to 2018)

The average cost for a data breach in India has gone up to INR 11.9 Cr (USD 1.7 Mn), an increase of 7.9% from 2017 with the **average cost per record being INR 4,552 (USD 64)**

BUSINESSES IN INDIA HIGHLIGHT 'CYBER INCIDENTS' AS THE TOP RISK (ALLIANZ RISK BAROMETER 2019)

RANK	
1	Cyber incidents (e.g.cyber crime, IT failure/outage, data breaches, fines and penalties)
2	Natural catastrophes (e.g. strom, flood, earthquake)
3	Business interruption (incl. supply chain disruption)
4	Market developments (e.g. volatility, intensified competiton/new entrants, M&A, market stagnation, markte fluctuation)
5	Changes in legislation and regulation (e.g. trade wars and tariffs, economic sanctions, protectionism, Brexit Euro-zone disintegration)

As threat surface continues to expand due to rising digitisation in the country, 'Cyber Risk' becomes pivotal in the overall risk management strategy. While most MNCs and large corporations (BFSI, IT-BPM, Energy sector) in India highlight the adequacy of their spending on cyber security products and solutions as a means to safeguard businesses, none can really assure complete security as attacks seem to get sophisticated by the day. And it is not only the large businesses; one of the recent bank attacks of 2018 highlighted the vulnerabilities of co-operative banks in India, bringing into picture that even small and medium businesses could be victims of attacks. For India, the road to becoming a USD 1 Tn digital economy by 2025 can only be achieved when a robust cyber risk mitigation strategy is in place.

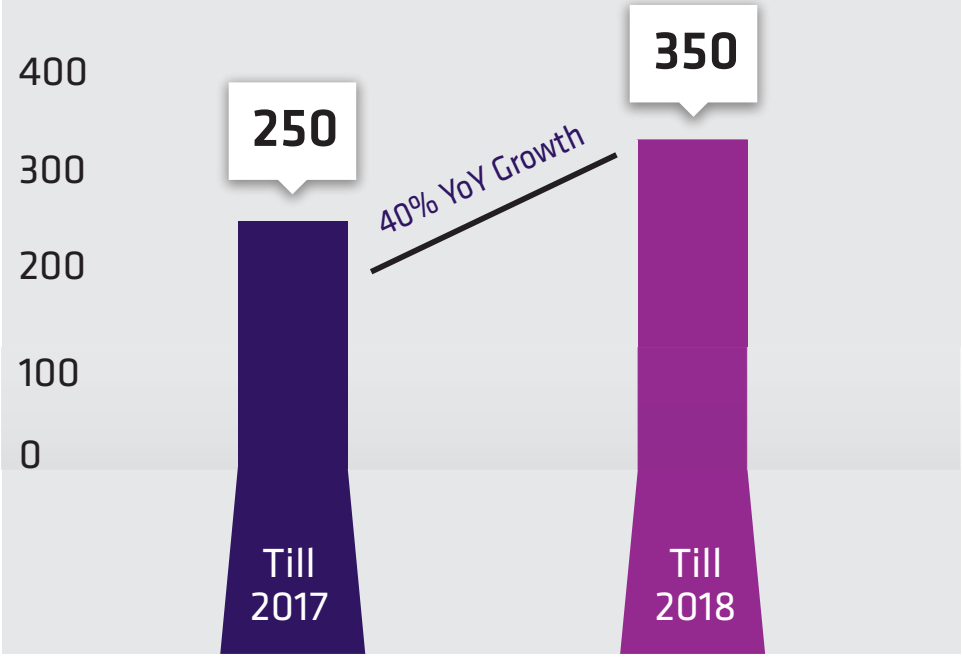
Source: MeitY Report on India's Trillion Dollar Digital Opportunity, 2019; NASSCOM Strategic Review FY 2018, Allianz Risk Barometer 2019, Symantec Threat Report, IBM-Ponemon Institute Study, Economic Times

CYBER INSURANCE IN INDIA

At a nascent stage with ~350 policies sold till 2018

To address cyber risks and provide a more comprehensive and meaningful cyber cover, Cyber Insurance as a standalone product was first introduced in 2014. Before that, cyber was (in some limited form) covered as endorsements under Professional Indemnity Policies, General Liability Policies, etc. Insurance providers also offer customizations based on sectoral and company-specific requirements, making it pertinent for the buyer to ask the right set of questions on coverage.

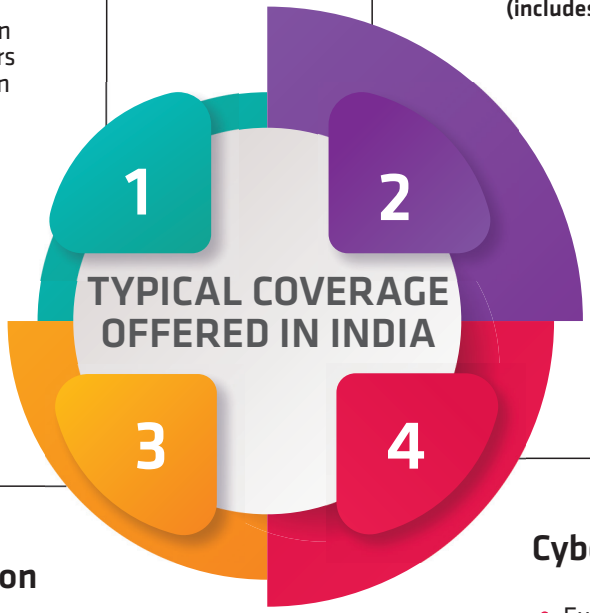
NO. OF CORPORATE CYBER POLICIES SOLD



Data aspects covered by cyber insurance

- Personal health information (PHI)
- Personally identifiable information (PII)
- Payment card information (PCI)
- Confidential third-party/research information
- Data hosting, outsourced electronic processing, or data storage

TYPICAL COVERAGE OFFERED IN INDIA



1st Party Expenses

- Regulatory Investigation & Fines (includes lawyers professional fees, admin costs, etc.) GDPR included
- Expenses:
  Forensic
  IT Audit
  Crisis Management
  (includes Stakeholder Notification, Legal Costs)
  Credit Monitoring
  PR & Media

Privacy & Data Liability
(includes 3rd party liabilities as well)

- Loss of Personally Identifiable Info
- Loss of Corporate Confidential Info
- Cover for Outsourcers
- Network Liability (such as DDoS Attacks)
- Multimedia cover (includes copyright issues)

Business Interruption

Income loss, business interruption costs, system damage and restoration costs, any extra expenses

Cyber Theft

- Fund Transfer Frauds
- E-Theft Loss
- E-Communication Loss
- Cyber Extortion

KEY INSURANCE PROVIDERS (Indicative List)

TATA AIG INSURANCE WITH YOU ALWAYS
ICICI Lombard
BAJAJ Allianz
दि न्यू इन्डिया एश्योरन्स कंपनी लिमिटेड
The New India Assurance Company Limited
HDFC ERGO

Source: YourStory, The Economic Times, Quora, Expert Insights

TOP TRENDS

Owing to market competition among carriers, premium amounts coming down

01 SECTORAL INSIGHTS

IT/ITes and Banking & Financial Services are early adopters

- Newer demands from manufacturing, pharma, retail, R&D and IP-based organisations, and hospitality
- Demands from IT companies due to contractual requirements, and GDPR

02 MARKET INSIGHTS

~350 cyber insurance policies sold till 2018, a 40% increase from overall base in 2017

- Yearly cyber premium in the range of **INR 80-100 Cr** (USD 11 to 14 Mn)
- 40-50% of policies bought by buyers opting for a cover of less than USD 5 Mn which includes builders, manufacturers, healthcare, SMBs etc.

03 PREMIUM

Premium amounts coming down, owing to competition among carriers for market share

- **For 1 Mn USD coverage**, premium amount ranges from **USD 6,500 – USD 8,000** (can be higher for banks and financial services; IT and pharma working in global markets; manufacturers with Industrial IoT)
- Premium amounts coming down owing to market competition

04 COVER

Insured amounts ranging from USD 1 Mn to USD 200 Mn

- Companies typically start with small cover, and gradually increase it
- Large IT services companies - max. **USD 200 Mn** coverage
- Large public/private sector banks – max. **USD 50-100 Mn**
- Manufacturing – max. **USD 14-15 Mn**

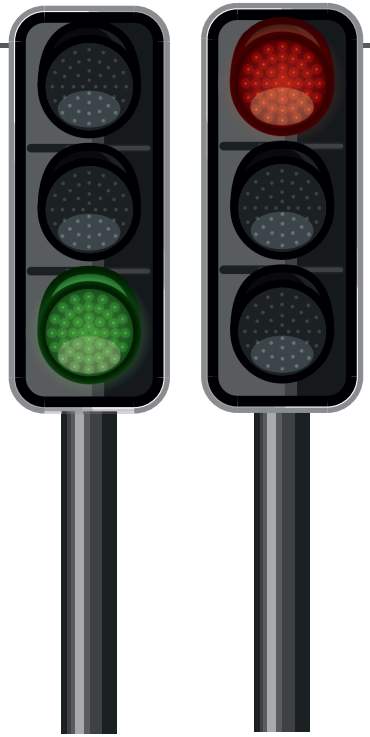
Source: Expert Insights; YourStory

DRIVERS & CHALLENGES

Evolving threat and regulatory landscape are key drivers

DRIVERS

- Rising digitalisation of businesses due to adoption of Cloud, Mobile, Social Media and IoT, thus, expanding the threat surface
- Evolving threat landscape, with the recent ransomware/malware attacks, targeting even the SMB sector
- Increasing awareness on cyber security
- Apprehensions around implications of GDPR and India's Personal Data Protection Bill (when it comes to effect)



CHALLENGES

BUYER

- Lower awareness on cyber insurance
- Enterprises finding buying and claim processes to be tedious
- Lack of understanding on which insurance policy to purchase

INSURANCE PROVIDER

- Lack of actuarial data on cyber attacks inhibits robust risk assessment
- Damages owing to cyber extortion, reputational loss, and rapidly evolving data and privacy landscape makes it difficult to quantify comprehensiveness and adequacy of cover
- Cut throat competition on premium amounts
- Gap between buyer's expectations for cover and what a carrier has to actually offer
- Buyers' reluctance on sharing data that can help carriers evaluate risks

DATA PRIVACY & PROTECTION

- The EU General Data Protection Regulation (GDPR) penalties that can go to a maximum of either EUR 20 Mn (~USD 22.75 Mn) or 4% of total worldwide annual turnover (whichever is higher) is prompting companies (particularly in the professional services sector) to consider cyber insurance. GDPR makes its applicability very clear - it will apply to the processing of personal data of EU individuals by controllers and processors, regardless of whether the processing takes place in the EU or not.
- However, a 2018 North American survey shows that 71% of respondents felt that GDPR may not have a significant impact on buyers unless there are headline losses.
- The anticipation of India's Draft Data Protection Bill is also prompting companies to talk about cyber policies, particularly those dealing with personally identifiable information, and processing financial transactions **(retail, fintech, eCommerce, BFSI)**
- The draft bill lays down penalties under chapter XI of the bill, ranging from INR 5 crore or two per cent of total worldwide turnover to INR 15 crore or 4% of the total worldwide turnover.

Source: Asia Insurance Review; SecureNow; Bank Info Security; PartnerRe & Advisen Trends Report; Aon White Paper

PERSONAL CYBER INSURANCE

As digital becomes pervasive, personal cyber insurance debuts in India

POLICY COMPARISON

FEATURES	HDFC ERGO E@SECURE	BAJAJ ALLIANZ CYBER SAFE
Eligibility	18+ years	18+ years
Sum Assured	INR 50,000 - INR 1,00,00,000	INR 1,00,000 - INR 1,00,00,000
Premium	INR 1,410 - INR 14,273	INR 662 – INR 8,993
Incidents Covered (Specified Events)	▸ Unauthorized online transactions ▸ Phishing & email spoofing ▸ Damage to e-reputation ▸ Identity theft ▸ Cyber bullying ▸ E-extortion	▸ Identity theft cover ▸ Social media cover ▸ Cyber stalking ▸ IT Theft ▸ Malware Attack ▸ Phishing and email spoofing ▸ Media liability ▸ Privacy and data breach by third party ▸ Identity theft ▸ Cyber extortion

Source: Bloomberg Quint; Naavi.org; Goodreturns.in; HDFC ERGO Documents; Expert Insights

STRATEGIC NEXT STEPS

Concerted efforts required, keeping buyer's perspective central

GOVT./REGULATORY BODIES/ASSOCIATIONS

- ✓ Creating awareness and ecosystem skills in cyber insurance policies
- ✓ Incentivize SMBs through direct intervention or providing procurement benefits
- ✓ Providing Toolkits and Checklists
- ✓ Creating an ecosystem for cyber insurance to mitigate risks & improve resilience
- ✓ Mechanism for Data Breach Notification
- ✓ Creation of Cyber Incident Data Repository
- ✓ Promoting actuarial science for better modelling of cyber risks

TECHNOLOGY FIRMS

- ✓ Establish sector-specific cyber risk assessment framework
- ✓ Innovate to offer tailor-made products & services for cyber risk evaluation, forensics, incident response etc.
- ✓ Fortify capabilities

BROKERS

- ✓ Spread awareness on essential coverage – create toolkits & checklists
- ✓ Support SMBs and startups, who wish to buy insurance policies
- ✓ Clearly articulate provisions under cyber insurance, and other insurance policies

INSURED/BUYER

- ✓ Engage with a technology firm for cyber risk evaluation
- ✓ Before buying, important to create a 'Cyber Insurance Committee' that has representation from Insurance Purchase Group, Offices of CFO, CEO, CIO/CISO, CRO and CMO, for better decision making

CARRIERS (INSURANCE PROVIDERS)

- ✓ Fortify technological capabilities or engage with third party to conduct pre-breach cyber risk assessment and post-breach assessment
- ✓ Digitize for data-driven decision making
- ✓ Prepare for comprehensive inclusion of data privacy & protection to cover regulations such as GDPR, India'a Draft Bill on Data Protection etc.
- ✓ Provide value-added services – customization, free counselling, trainings etc.
- ✓ Clearly articulate provisions under cyber insurance, and other insurance policies

Source: Expert Insights; Department of Homeland Security, US

BUYERS' CHECKLIST & QUESTIONS

Ask the right set of questions for better policies

- What aspects are covered under 'Cyber Insurance'? Is there any overlap with other traditional insurance?
- Does the policy offer pre-breach cyber risk assessment? Are there provisions for annual premium adjustments?
- Does the policy have a panel of suppliers for post breach cover – forensic companies, PR, legal etc.?
- Does the policy offer full limits for all coverage?
- Does the policy cover laws of foreign countries, where you have business, such as GDPR?
- Does the policy have a single retention and not separate retentions for each coverage element?
- What is the minimum waiting period for business interruption cover?
- Does the policy mention inclusion of GDPR coverage with full policy limits, to the extent insurable by the law?
- Are voluntary notification costs included in event management language?
- Does the policy include cover under rogue employees?
- Is terrorism specified in the policy, and what does it cover?
- Does the policy provide access to extortion advisors?
- Do suppliers have to be listed on the policy for coverage to apply?
- Is it possible to have firms added to the pre-agreed panel?
- What are the exclusions?

CYBER INSURANCE CHECKLIST

PRE-BUYING REQUISITES

- Engage with a third party (broker/tech provider) to self evaluate, upgrade, identify the right set of carriers, and get better deals on premiums
- Before buying policies, create a 'Cyber Insurance Cross-Functional Committee' that has representation from Insurance Purchase Group, Offices of CFO, CEO, CIO/CISO, CRO and CMO for better decision making

Source: Preparing for Cyber Insurance by Insurance Europe; Expert Insights

INITIATIVES PLANNED FOR DSCI MEMBER COMPANIES

DSCI
PROMOTING DATA PROTECTION
A NASSCOM® Initiative

CYBER INSURANCE - INITIATIVES PLANNED FOR MEMBER COMPANIES

1. Creating awareness through workshops, expert sessions and consultations
2. Providing Toolkits & Checklists
3. Member deliberations and chapter meetings to identify and explore cyber insurance as a means to improve cyber resilience
4. Using cyber insurance as a lever to create SMB-specific cyber toolkits
5. Encouraging Indian technology firms to offer tailor-made products & services for cyber risk evaluation, forensics, incident response, data analysis, etc.

A **NASSCOM®** Initiative

DATA SECURITY COUNCIL OF INDIA
3rd FLOOR, NASSCOM CAMPUS, PLOT NO. 7-10, SECTOR 126, NOIDA, UP-201303

For any queries contact
P: +91-120-4990253 | E: info@dsci.in | W: www. dsci.in

data-security-council-of-india DSCI_Connect dsci.connect dscivideo