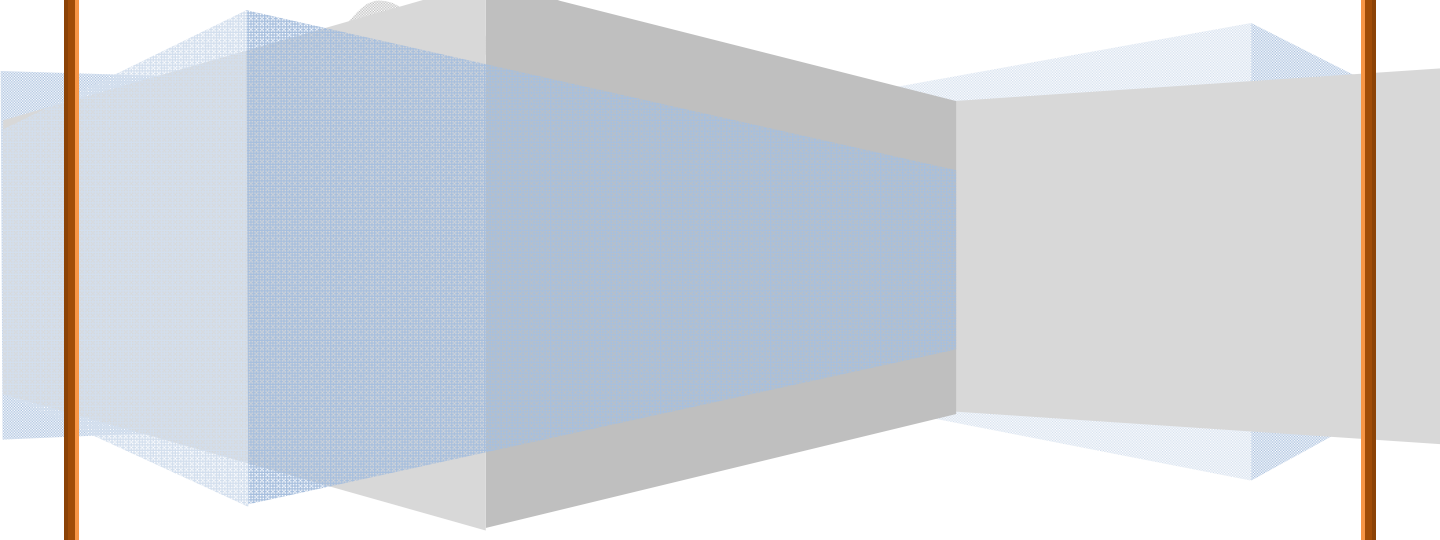
JK RISK MANAGERS AND INSURANCE BROKERS LTD

Cyber & Technological Risk

Cyber Liability insurance



Cyber & Technology Liability in India

Scenario in India: Cyber risk insurance seems to take an uptick

Recent data indicate that India is ranked third globally in terms of vulnerability to cyber attacks, accounting for 6.5 per cent of the targeted attacks in 2012.

Some high risk sectors are banking and information technology as they handle and process large amounts of personal and proprietary data for their customers on online platforms. There are also concerns on the likely impact on the outsourcing industry which depends upon work from overseas companies.

Two Indian technology firms, working as outsourced payment processors, were in the spotlight recently for their alleged role in a $45-million credit card fraud impacting Indian and international banks. In another incident, cyber criminals reportedly hacked into an RPG group company's bank account and siphoned off INR 24 MLN through the real time gross settlement system (RTGS).

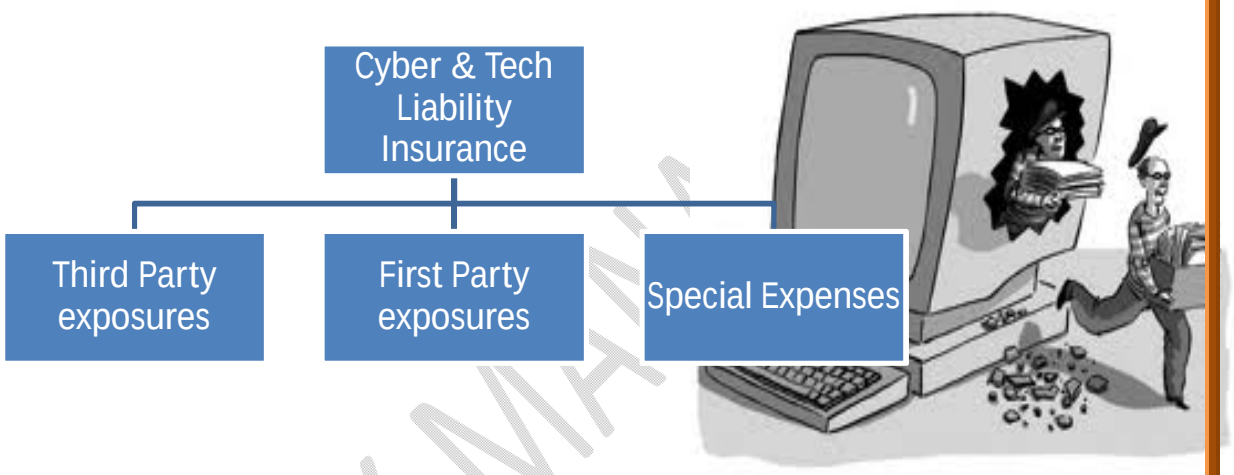
TARGET MARKET

The product is aimed at a wide range of companies as most businesses have an exposure to cyber

Some industry examples include:

- Website operators and e-tailers
- Healthcare providers
- Leisure and entertainment companies
- Software companies
- Manufacturers and wholesalers
- Financial Institutions like Bank, NBFC, etc
- Manufacturers and wholesalers
- Professional service companies

Cyber & Technology Liability



Coverage:

Claims against Insured's (Third Party exposures)

Negligence:

Negligent act, error, omission, misstatement, misrepresentation, breach of an express or implied contractual duty to use reasonable care and skill including negligent supervision of an employee or sub-contractor or any other negligent conduct of the Insured or any sub-contractor or consultant supplied to the client for whom the Insured is legally liable;

Infringement of intellectual property:

Infringement, breach, violation, wrongful use, misuse, misappropriation, passing off, plagiarism, piracy or dilution of any: copyright, trade dress, trademark, trade name, service mark, service name, registered or unregistered design, slogan, title, web domain name, database, title, sound, voice, name, likeness, identity, music, or other artistic or creative work, including violation of creator's moral or attribution rights, publicity rights, ideas under implied contract including liability for infringement of intellectual property rights that the Insured has assumed through an indemnity provided through a written contract between the Insured and their client for the provision of Computer Hardware, or other Deliverables, including unfair competition when alleged in conjunction with any of the preceding;

Breach of contract:

Unintentional breach of a written contract to provide services or Deliverables in the course of Your Technology Activities by reason of those services or Deliverables failing materially to conform with any agreed written specification or delivery timescale that forms part of the relevant contract, or failing to meet any agreed or implied industry or statutory term concerning quality or fitness for purpose

Invasion of privacy:

Invasion, intrusion, infringement or interference with rights of private occupancy, privacy or publicity, including trespass, wrongful entry or eviction, eavesdropping or harassment, false light, commercial appropriation of name or likeness, disclosure of private personal information, breach of any duty of confidence or confidentiality;

Defamation:

Defamation including libel, slander and trade libel, product disparagement, injurious or malicious falsehood, infliction of emotional distress or outrage due to harm to the character, feelings or reputation of any person, entity or organization.

Advertising:

Unintentional misrepresentation in advertising or any unintentional breach of any comparative advertising regulation or statute;

Breach of license:

Unintentional breach of licence of Third Party's trademarked or copyrighted material in terms of period, territory or medium of use;

Breach of Confidentiality:

Unintentional breach of an agreement to maintain the confidentiality of a contributor or source of material or failure to portray someone or a subject in a certain light or to credit or attribute authorship, and the reliance of others on that agreement to their detriment

False arrest:

Malicious prosecution, abuse of process, false arrest, detention or imprisonment

Dishonesty:

Fraud or dishonesty of any Employee or contract staff

Bodily injury or property damage:

Bodily injury or property damage arising directly from any negligent act, error, omission, misstatement, misleading statement or misrepresentation in Content by You solely in the conduct of Technology Activities

Unauthorized access and social engineering:

Failure to prevent unauthorized access to, unauthorized use of or tampering with data or systems or any unauthorized access to or posting on a website, including the use of social engineering techniques, via the Insured Computer System or a computer network your control or manage on behalf of a Third Party

Computer virus:

Unintentional introduction or transmission of malicious code or computer virus into data or systems

Denial of service:

Failure to prevent denial of service attacks on a computer network you own, control, or manage on behalf of a Third Party

Loss of documents or data:

Destroyed, damaged, lost or mislaid documents or Electronic Data held on the Insured Computer System or in transit

Multi-media liability:

If you infringe a third party's intellectual property rights(other than patents – cover can be arranged for this separately through our Intellectual Property Policy),defame them, breach their privacy or commit any negligence in the publication of any content in electronic or print media, we pay for your investigation and defence costs, as well as any civil damages.

Insured's' own losses and expenses (First Party Exposures)

Business Income Loss and Expense:

Business Income Loss and Expense in excess of the Retention and subject to the Time Retention, as the direct result of :

1. A system Failure caused by an Unplanned Infrastructure Event which both first occur during the Policy Period;

2. Unauthorized copying, distribution or dissemination of data including Electronic Data following Unauthorized Access to the Insured Computer System;

3. The withdrawal of credit card processing facilities following any official action or investigation by or decision or order of the Payment Card Industry as a result of Unauthorized Access to, theft or accidental loss or release of Personal Information that results in a breach of the Payment Card Industry Security Standards;

4. Seizure of the Insured Computer System by a government body arising out of Content in connection with Your Technology Activities

Data Restoration:

Data Restoration Costs incurred by the Insured in the event it is discovered during the Policy Period that Electronic Data or Software on the Insured Computer System is lost, damaged, deleted, destroyed or corrupted as the result of an Unplanned Infrastructure Event.

Crisis Management:

To protect the reputation of the Insured, and/or investigate and take corrective action, following an Unplanned Infrastructure Event.

Disputed Fees:

Disputed Fees serve to avoid a Claim covered under Coverage Agreement A in respect of Your Technology Activities.

Extortion

Extortion Expenses and Extortion Losses as the result of any Extortion Threat first made against you.

C. SPECIAL EXPENSE

Indemnification is extended with Insurers' prior consultation and written consent for legal expenses incurred by you during the Policy Period in the course of Your Technology Activities in responding to or complying with:

Regulatory Action:

Any official action or investigation by or decision or order of any regulatory body with responsibility for your industry in connection with Your Technology Activities;

Payment Card Industry:

any official action or investigation by or decision or order of the Payment Card Industry following Unauthorized Use, Unauthorized Access to, theft or accidental loss or release of Personal Information which results in a breach of Payment Card Industry Data Security Standard.

Premiums & retention

A range of deductibles available, from as low as USD 1,000. The deductible will depend on risk to risk.

- Premiums starting from as little as $300 for a$1,000,000 limit

Metrics used for underwriting

- Geography
- Industry sector
- Company revenue

Myths busted on the protection of DATA Losses:

General Liability (GL)

A GL policy will only cover bodily injury and property damage losses and, as data is deemed by the courts to be an intangible form of property, no coverage would usually be provided for breaches of privacy. Although attempts have been made to claim that a 'hack' is 'trespass' under a GL policy, this argument has met with limited success.

Property:

Property insurance will typically only cover damage to tangible property. As explained above, data is deemed by the courts to be an intangible form of property, so no coverage would usually be provided for damage to data. Also, whilst you may have coverage for business interruption arising out of material damage, you will not usually have cover for business interruption arising out of non-material damage to your network. Computer viruses and network exposures are typically excluded specifically.

Computer All Risks:

This insurance covers you for costs involved in repairing damaged hardware (tangible property) and would not respond to claims for lost data that are covered under the Cyber insurance.

Claim Scenario Worldwide

Large companies that have been recently badly affected by IT & Technology related risks:

- RBS- Royal Bank of Scotland :
  - In June 2012, a corrupted software update at The Royal Bank of Scotland caused significant business interruption over a 5 day period. The corrupted file was applied to the payment processing system, leaving customers unable to withdraw cash from ATMs or to view their account details. Wages were disrupted and the system was unable to process direct debits.
- E-bay- e-commerce firm
- Cisco systems
- RIM, a Canadian company :
  - Any Blackberry user recalled the global technical hitch in 2011 that hit Canadian Company RIM, when users of their BlackBerry devices were unable to access email for several days.
- Amazon

Cyber Risks underscored: A German retailer's network suffered interruption during a denial of service attack and was down for 48 hours. Although there was an increase in sales following the network being brought online again, it was not enough to fully cover the lost sales during the downtime. Insurers investigated and paid for d2.5m of income loss, as well as d250k of redundant fixed operating expenses that were incurred during the downtime.

Costly financial impact

The financial cost of cyber attacks is enormous and growing. Cyber threats cost companies in terms of impact on operations and lost productivity, legal costs, lost intellectual property, and in reputational damage. In fact, AIG found the average security and privacy claim size was $5.2 million. The cost is real, as the Sony Corporation discovered in 2011 when its PlayStation network was maliciously breached. The breach resulted in a 23-day closure of the PlayStation online network and Sony suffered an estimated financial loss of $171 million and a 55% drop in its share price in the four months following the breach.

It is no coincidence that the World Economic Forum ranked cyber risk as the single largest threat to global infrastructure for 2012, above financial collapse, natural disaster or traditional terrorism. Cyber threats are real, growing, and very costly.

Scenario in India

Recent data indicate that India is ranked third globally in terms of vulnerability to cyber attacks, accounting for 6.5 per cent of the targeted attacks in 2012.

Some high risk sectors are banking and information technology as they handle and process large amounts of personal and proprietary data for their customers on online platforms. There are also concerns on the likely impact on the outsourcing industry which depends upon work from overseas companies.

Two Indian technology firms, working as outsourced payment processors, were in the spotlight recently for their alleged role in a $45-million credit card fraud impacting Indian and international banks. In another incident, cyber criminals reportedly hacked into an RPG group company's bank account and siphoned off Rs 2.4 crore through the real time gross settlement system (RTGS).

Cyber Risks underscored: Approximately 300,000 customer credit card numbers were stolen from an online retailer by a hacker, who then tried to use the stolen information to extort $100k from the company. When the company refused to co-operate, the hacker posted tens of thousands of card numbers online. The online retailer suffered approximately $2,000,000 in lost income and third party damages as a result of the credit card companies' cancelling and reissuing cards.

Way Ahead

In the developed world, governments have started bringing in legal and regulatory frameworks.

These involve large fines and penalties for an entity in the event of a cyber breach. For instance, the European Union Privacy Directive provides that companies that violate European data protection rules may be fined up to €1 million or up to 2 per cent of their global annual turnover.

In India, the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011, an amendment to the IT Act, 2000, enforces a criminal liability of imprisonment for two years and a civil liability of a fine of INR 100,000 or both for a breach.

In addition, the Reserve Bank of India has directed banks in India to insure themselves against cyber risks.

Increased government attention can lead to more comprehensive laws, with implications of higher penalties, to reflect global trends.

Thus requirements of insurance products are paramount to safe guard one self and continue their businesses.

The Cyber liability and JK Risk Managers technical nouns:

The ever growing spurt of cyber crime has been a cause of grave concern for organizations across the frontiers. The risk has drawn the global attention after so many cyber debacles and 'SNOWDEN' effect has just added to the hue and cry.

JK Risk Managers has sniffed at the problems, and the gap of the industry requirements and the coverage available in the market. This has spurred JK Risk Managers to look beyond the Indian cauldron and reach other shores to close the gap. In addition, we can work in tandem with you and suggest how you can make yourself safer and tackle this menace.

What we need to know primarily:

- Your revenue
- Geographical location
- Business profile
- Nature of Industry
- Does business transaction with US-domiciled companies

Our address:

JK Risk Managers & Insurance Brokers Ltd.
A-21
Sector -5, Noida – 201301
Phone No.: +91 120 -4965100

JK Risk Managers & Insurance Brokers Ltd.
3rd Floor, Kasturi Bulding
7, Jamshedji Tata Road
Churchgate, Mumbai 400 020
Phone No.: +91 22 – 22040794/96

To Stay tuned to us is to stay secure