CYBER INSURANCE:
A STRATEGIC APPROACH TO RISK MANAGEMENT

Key Trends:

- Cyber-crime is the primary concern for companies of all sizes in different parts of the world, including the Americas, Africa, the Middle East, Asia Pacific, and Europe.
- In 2023, India recorded 2,138 weekly cyber-attacks per organization, a 15% increase from 2022.
- Hackers are using artificial intelligence (AI) powered language models to increase the speed and scope of ransomware attacks
- The Indian automobile industry emerged as the primary target of cyber-attacks in 2023
- Smaller companies are more vulnerable and prone to a cyber-attack due to weak processes and system.

Cyber threats like ransomware attacks, data breaches, and external threats to the IT systems stand out as primary global risks. Hackers are increasingly directing their efforts towards both IT and physical supply chains, initiating widespread cyber assaults, and developing new methods to extort money from enterprises of all sizes.

Looking ahead to 2024, AI-generated voice and video scams are emerging as significant threats, alongside the manipulation of realistic fake data. Deep fake technology further complicates matters, making it difficult to discern authentic communications from fabricated ones. Social engineering fraud, empowered by these advancements, poses a potent risk to individuals and organizations, underscoring the critical need for robust cyber-security measures and heightened awareness. Businesses must adopt proactive risk management practices, and consider cyber insurance given the escalating cyber threats.

Ransomware and malware emerge as the most rapidly increasing threats of 2024.

Malware Attack

- Dominant Threats: **41% Trojans** & **33% Infectors**
- Geographical Hotspots: **15% Telangana** & **14% Tamil Nadu**
- City-wise Analysis: **15% Surat** & **14% Bengaluru**

Top Affected Industries:

Automobile | Government Entities | Education Sector

Ransomware and Cyber Extortion

- 2023: **235,472** ransomware incidents across India
- 2023: **77%** of Indian Companies Victim of Ransomware Attack in India
- **Main Causes:** Exploited Vulnerability: **35 Percent Cases**
- Compromised Credentials: **33 Percent Cases**

Only 20% Industries are equipped with a formal plan to deal with ransomware attacks.

Top Affected Industries:

Health Care Industry | Manufacturing Industry | Government Entities

Case Studies:

FINANCIAL SERVICES:

There have been numerous instances in which hackers have withdrawn substantial sums from customers' accounts by infiltrating the bank's ATM server, employing skimming devices to pilfer cardholders' details.

HEALTH CARE SECTOR:

An Indian healthcare website fell victim to a cyberattack, where hackers breached security measures and accessed records of both patients and doctors.

E-COMMERCE SECTOR:

An e-commerce company disclosed experiencing a data breach, during which personal details of customers, including email addresses, full names, and IP addresses, were compromised.

MANUFACTURING:

Manufacturing industry today are increasingly dependent on digital networks. The dependency is only going to increase with the advent of AI and Generative AI models. The infrastructure network of manufacturing companies are vulnerable to threats that can lead to significant downtime of their operations causing “Loss of business revenue”. The supply chains with large repositories of sensitive data have also become lucrative target for cyber attacks. Many cyber attacks in the manufacturing industry are a result of vulnerabilities in their supply chain which has caused large financial losses to them.

Cyber Insurance Overview:

Cyber insurance is a type of insurance policy designed to protect businesses and individuals from first-party and third-party losses or damages resulting from cyber-related incidents. It typically provides financial reimbursement for expenses related to incident response, data recovery, legal fees, and any other costs associated with mitigating the impact of a cyber incident. Cyber insurance policies vary in coverage and can be tailored to the specific needs and risk profiles of the prospective insured.

Coverages:

Repair of Company and Individual Reputation: covers the professional fees, and expenses of independent advisors, who can prevent or mitigate the potentially adverse effects of a newsworthy cyber event.

Network Interruption: covers the loss of net profit as a result of a material interruption to the insured's network, as a result of a security breach.

Cyber/Privacy: coverage protects against financial losses incurred from threats or demands made by cyber-criminals, including ransom payments and related expenses.

Notification and Monitoring: covers the costs incurred for notifying the customers (or any relevant regulatory authority), that their data has been affected by a breach. The policy covers a reasonable costs and expenses associated with it.

Multi-media Liability: covers claims from third parties arising solely from the execution or omission of multi-media activities, including alleged or actual wrongful acts such as defamation, intellectual property infringement, plagiarism, and liability resulting from the insured party's negligence concerning any digital media content.

Data Liability: covers the damages & defense costs associated with a breach of personal or corporate data, whether caused by the insured or their outsourced data-handling firm.

Privacy and Data Breach: is a type of coverage that provides financial protection to individuals or organizations in the event of a data breach or unauthorized access to sensitive information, covering expenses such as, forensic investigations, notification costs, legal fees, and damages resulting from third-party claims.

A. First Party Cost Includes:

- Data Administrative Fines
- Reputational Damage Costs
- Data Restoration Cost
- Network Security
- Privacy and Data Breach Cover

Optional Extensions Include:

- Cyber/Privacy Extortion
- Network Interruption

B. Third Party Liability Includes:

- Network Security
- Privacy and Data Breach Cover

Optional Extensions include:

- Multi-media Liability

Exclusions:

Below are some of the primary exclusions. For a comprehensive list of exclusions, please refer to the policy documents.

Prior claims and circumstances | **Any dishonest or improper conduct** | **Bodily Injury/ Property Damage** | **Critical Infrastructure** | **Crime Insurance**

Like all other liability insurance policy, cyber insurance policy also attracts deductibles per claim incident.

Sources: Allianz Report, Business Today, India Today

TATA MOTORS INSURANCE BROKING AND ADVISORY SERVICES LIMITED

Composite Brokers License No. 375 I Validity 13/05/2023 to 12/05/2026 I CIN: U50300MH1997PLC149349
Corp Office: 1st Floor AFL House, Lok Bharti complex, Marol Maroshi Road, Andheri (East), Mumbai - 400 059. Maharashtra. India.
Registered Office: Nanavati Mahalaya, 3rd floor, Tamarind Lane, Homi Mody Street, Fort, Mumbai - 400 001. Maharashtra. India.
A sister Company of TATA AIA Life Insurance Company Limited and TATA AIG General Insurance Company Limited