Cyber Risk Insurance

Insurance Policy to cover financial liabilities arising from cyber incidents

Edited by **MOHAN DAS VISWAM**

Digital revolution has transformed the way individuals and communities act, interact and transact. No other scientific advancement, perhaps, has made inroads among all cross sections of the society in such a short span of time. While the envisaged dividends of this advancement are amazing, the associated risks and costs are also equally enormous. Data being the new oil, cyber criminals are burning the midnight oil to take advantages of any failure of the people, process or technology associated with this revolution. Even the slightest failure in ensuring the security of the data and associated services is a luxury that no individual or organization can ever afford.

Cyber threats are a constant concern for organizations of all nature. The assumption that commercial establishments such as banking and financial institutions alone are prone to such threats is a misnomer. Organizations in other sectors such as energy, healthcare and aviation are also equally, often even more, getting susceptible to cyber-attacks. Hence the data owners are under constant vigil with the right tools and expert manpower in place to protect the organization's sensitive information and assets. Any lacuna from their end in protecting the interests of the customers will cause an irreparable loss in business and of reputation to the agencies concerned.

CJ Antony
Dy. Director General & SIO
antony@nic.in

Cyber Risk Insurance, also simply known as Cyber Insurance, is a kind of insurance policy which protects business houses as well as individuals from financial losses due to cyber-related incidents. These incidents include various forms of cyber-crimes such as data breaches and cyber-attacks. The policies usually cover costs associated with extortion payment, restoring data and systems, legal fees, and liability for damages to third parties. Cyber insurance protects businesses to manage cyber risks and safeguards them from potential financial losses.

Losses due to cyber-attacks are often intangible and difficult to quantify. Impalpable losses like that of reputation and leak of intellectual property will be slow in taking its toll on the prospects of the organization. The assessment of tangible losses is also difficult as the spread and depth of the damages takes time to get revealed. These losses need to be filled as and when they are revealed for ensuring mere business continuity. Besides, clients and other stake holders are likely to seek compensation for denied services, loss of personal information and other collateral damages. All these may throw the organization into deeper financial turmoil which will be difficult to circumvent without external support.

Cyber Risk Insurance

Cyber risk insurance helps business establishments to manage the risks associated with cyber-attacks. It is a special insurance product that covers liabilities related to information technology infrastructure and activities that are normally not covered by other insurance products. It protects the organisations against the potentially devastating financial consequences of data breaches. It provides a smooth funding mechanism to recover from major losses without any assistance from other sources such as banks and government agencies. Thus it helps businesses to return to normal in a short period of time in the event of a large-scale security breach.

Liabilities Covered

Cyber insurance, like other insurance products, provides coverage for various kinds of liabilities to the stake holders associated with the business. The coverage of cyber insurance policies typically includes the costs associated with extortion payment, restoring data and systems, legal fees, and liability for damages to third parties. The policies can be further customized to suite the specific requirements of the organisations. The major liabilities covered for the first, second, and the third parties are listed below.

Theft and Loss

Cyber Risk Insurance provides protection against costs of theft or destruction of the insured data. This enables organisations to compensate for the possible losses out of destruction of the data insured. Further it provides compensation for theft of the funds insured under the policy. This includes recompense for funds directly lost by banking and other financial institutions due to cyber-attacks.

Cyber Extortion

Payment of extortion money is not generally recommended in case of ransomware attacks. However, recovering from such attacks may sometime require payment of ransom. Cyber insurance provides compensation of expenses towards payments to extortionists who encrypted the data and/or threaten to disclose sensitive information. The cost of hiring the services of a professional negotiator is also covered under such insurance policies.

Business Interruption

Loss of income due to actual or potential impairment or denial of operations in the aftermath of cyber-attacks is a major concern for many business establishments. Cyber insurance covers the loss of income as well as the extra expenses incurred during the recovery period.

Response Cost

Businesses sometimes find it difficult to cop-up with the expenses for Forensic Investigation to assess the spread and depth of the attack following a security breach. As a result a complete root cause analysis is often avoided and the security holes are left unidentified and unattended. Cyber insurance comes to the aid of such organisations so that the chances of recurrence of similar security incidents are minimised.

Legal Recourse

Cyber insurance policies provide reimbursement of expenses towards legal advice and regulatory compliance in the wake of a cyber incident. This includes cost of determining indemnification obligations in the contracts of the organisations with a third party. Policies also provide indemnity against violation of privacy laws caused by a security breach.

Public Relation

Media handling is a vital activity in management of any crisis. Cyber insurance policies can be customized to include the cost of handling reputation attacks in the event of a security breach. The expenses to mitigate any negative publicity and cyber defamation due to the security incident are also often covered by such policies.

Notification Expenses

This includes the costs of notifying third parties potentially affected by a security breach. This often deserves importance considering the vast extend and strategic nature of the clientele of the affected organisation.

Privacy Liability

Cyber insurance policies provide indemnity against third-party damages that result from the disclosure of confidential information handled by the insured. This also includes coverage for vicarious liability where a vendor loses information the insured had entrusted to them.

System Liability

Damages that result from the failure to protect the electronic data of a third party during a cyber-attack is a major cause of concern for many organisations. Policies provide coverage for defense costs for which the insured is liable for third-party damages.

Access Liability

Businesses often may have to compensate for denial of services to the clients in the wake of cyber-attacks. Insurance policies provide indemnity from claims resulting from unavailability of IT systems to such customers.

Source of Cyber Threats

Cyber threats can emanate from internal as well as external source, and insurance policies usually provide coverage for such threats irrespective of their source and cause. Ignorance and negligence of employees are the most common cause of internal threats. Lack of awareness and training among employees causes improper handling of

systems which may ultimately pave way to cyber-attacks. Negligence among employees may lead to serious security issues such as misconfiguration of systems and loss of credentials and even the devices. Malicious and disgruntled employees are another common cause for internal threats which may lead to loss of data and denial of services.

Ransomware attacks are the prominent form of external threats covered under cyber insurance. There exists a cyber-crime business model called Ransomware as a Service where malicious elements hire the services of operators who are technically skilled to develop malware and launch ransomware attacks. State and non-State Hackers as well as Hacktivists form another major source of cyber-attacks which jeopardizes the services of any business house. Corporate espionage and malicious stakeholders (such as vendors in supply chain) are also serious cause of concern for many organisations. Proper risk assessments and contractual agreements will enable businesses to function in a realistic environment.

Side Benefits

Cyber Risk Insurance has a couple of side benefits as well. A comprehensive security audit of the digital assets is one of the pre-requisite for the candidate organisations to avail the coverage of the risk insurance. This effort will help the entities to determine the existing vulnerabilities and to undertake necessary remedial measures to fix those vulnerabilities. This process in-turn improves the security posture of the organisation and reduces the chances of security incidents.

A qualitatively superior and quantitatively accurate assessment of risk is another prerequisite to arrive at the premium of cyber risk insurance policies. This exercise distributes risks fairly among all the parties involved and avoids concentration of risk with any one of the stakeholders. This ultimately will put an end to free-rides by some players and burden each one with their share of risk. Ensuring security audit and risk assessment, whenever the insurance policies are renewed, will maintain the organisation in a healthy condition vis-a-vis cyber security and financial stakes.

Conclusion

With the increasing frequency of cyber-attacks, it's more important than ever to have the right people, policies and technologies in place to protect organization's sensitive information and assets. It is increasingly becoming important to establish a backup mechanism to shoulder the financial burdens of any such attacks. Like any other insurance product, consumers feel the premium spent on cyber insurance policies as a wasteful expenditure until they once claim the benefits of the same. While every endeavor may be made to secure one's data by deploying appropriate cyber security solutions, the benefit of an insurance policy that provides coverage for financial liabilities arising from cyber incidents also may be simultaneously ensured for a healthy and peaceful business atmosphere.

Contact for more details

C.J. Antony
Deputy Director General & SIO
NIC Tamil Nadu State Centre
E-2-A, Rajaji Bhavan, Besant Nagar, Chennai - 600090
Email: antony@nic.in, Phone: 044-2490 8001