Deloitte.

Cyber Insurance for Enterprises

For Private circulation only

Risk Advisory

Cyber Insurance for Enterprises

The wave of emerging technologies has had a pressing impact on the business environment. The business risks associated with these technologies pose a big threat to organisations. In terms of economic losses, the impact of a cyberattack could be as magnanimous as a natural disaster. While it is the most pressing risk for organisations, the World Economic Forum's Global Risk Report 2019 ranks cyberattack significant only after huge risks such as weapons of mass destruction, natural disaster, climate change, and water crisis.

Today, cyber incidents lead to multi-million dollar losses for organisations. With the attacks growing in number, sophistication, and impact, cyber breaches recorded by businesses have almost doubled in five years

Year	Breaches
2012	68
2017	130

Source: Identity Theft Resource Center

As per the Cost of Cyber Crime Study by Accenture, the average financial impact to companies for one or more cyber incident is US$11.7 million. Many organisations have realised that a cyberattack is inevitable – it's only a matter of time that an incident may occur.

The impact of cyberattacks goes beyond incidentals. The lack of established conventions and understanding of incident response makes it difficult to account for the overall impact that it may have on businesses.

These cyberattacks have significant financial consequences that vary by geography, industry, and sophistication of attack as detailed below:

In 2018, the average cost of a data breach was US$3.86 million dollars.

Based on multiple analyst reports, average cost per compromised record was around US$1,481.

In addition, there are other non-monetary risks such as reputational and regulatory risks.

Accepting or treating cyber risks always leaves residual risks that may create a wider impact

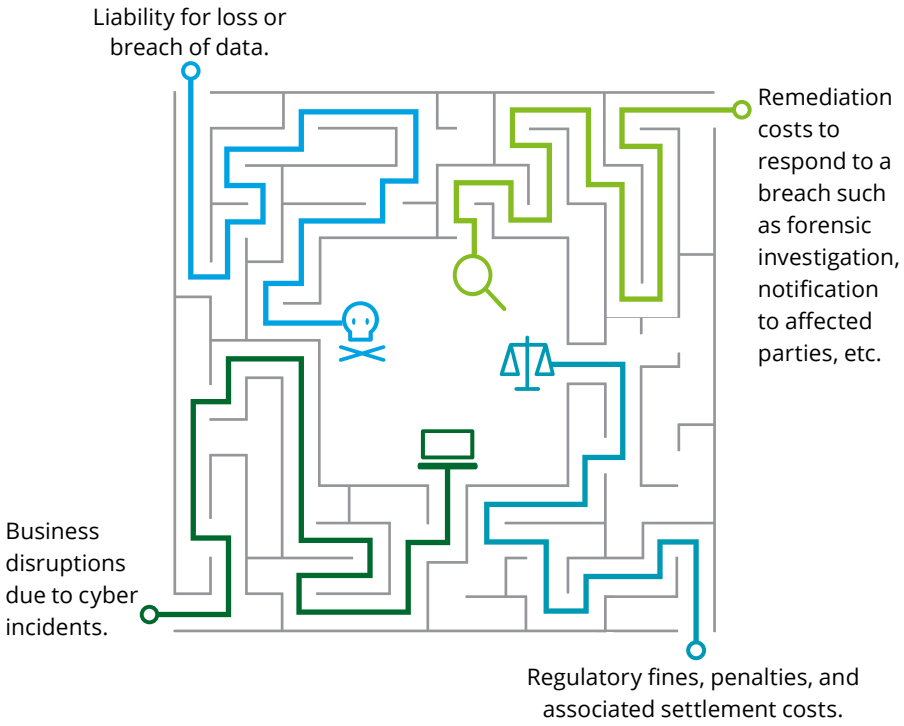
Source: IBM

The imperative

Across the world, organisations buy insurances to protect themselves against traditional risks, the growing number of attacks have helped us successfully conclude that cyber insurance is an imperative. In the short run, it covers an organization with respect to cyber risks. However, in the long run it ensures business sustenance in this volatile business environment.

An organisation can successfully mitigate losses arising from multiple cyber risk exposures. Depending on the nature, complexity, and maturity of an organisation's cyber risk posture, cyber insurances can cover losses associated with data breaches, compromise of confidential information, and even business disruption.

A good cyber insurance coverage can complement an organisation's active security programme by providing insurance coverage in the following broad areas:



Cyber Insurance: The Indian context

As per FICO, a data analytics company, the current Indian cyber insurance market is positioned at INR 300 million and is expected to grow up to INR 750 million by 2020. The number of cyber insurance policies purchased has grown. In the last four years, the number of policies purchased have increased by 25 percent and is likely to increase by another 30 percent, post the implementation of Privacy and Data Protection Act, India.

More and more Indian companies are opting for cyber insurance to protect themselves from forensic costs, cyber extortion costs, and other third-party coverages. Despite this, only 44 percent of Indian companies believe that their premiums are based on an accurate assessment of their company's risk profile.

Challenges to buy a Cyber Insurance

Rising number of incidents, inadequate response infrastructure, lack of awareness, and talent pool are all factors attributing to the growing need for cyber insurance. Despite this promising market opportunity, various barriers inhibit large-scale participation for hesitant buyers.

Lack of understanding of insurance coverage options:
Limited clarity on types of cyber risks covered under cyber insurance and amount of coverage required along with associated premiums.

Existing cyber insurance policies lack standardisation:
Buyers are unclear over how much exposure is actually covered. Aspects such as description of coverage terms, conditions, and exclusions are not standardised in cyber insurance policies. Similar products from different providers have varied features that make value and price comparisons a challenge.

Lack of relevant artefacts or references:
Since cyber-coverage claims and disputes have not reached critical audience yet, there is lack of references that leave buyers uncertain over success ratio of the claims settlement process

Implementing security controls versus purchasing a cyber-insurance:
Buyers are unsure of cost-benefit analysis of mitigating or transferring cyber risks to an insurer.

Claims litigation uncertainties:
Buyers fear claim litigation uncertainties that arise from differences over which policy applies, or whether policy language indicates coverage. This leads to difficult claims management and settlement of disputes.

Cyber risk can be spread over a wide range of coverage:
Cyber insurance buying process can be complicated, as buyers need to assess coverage needs and match policies with exposures, while also comparing alternatives. This can raise uncertainty over what coverage is required vs. what the organisation may already have in existing policies.

Cyber Insurance considerations

Prior to purchasing cyber insurance, organisations should understand all aspects of coverage and carefully consider what the policy terms include and exclude.

Here's a checklist of what a typical cyber insurance can cover in terms of financial assistance.

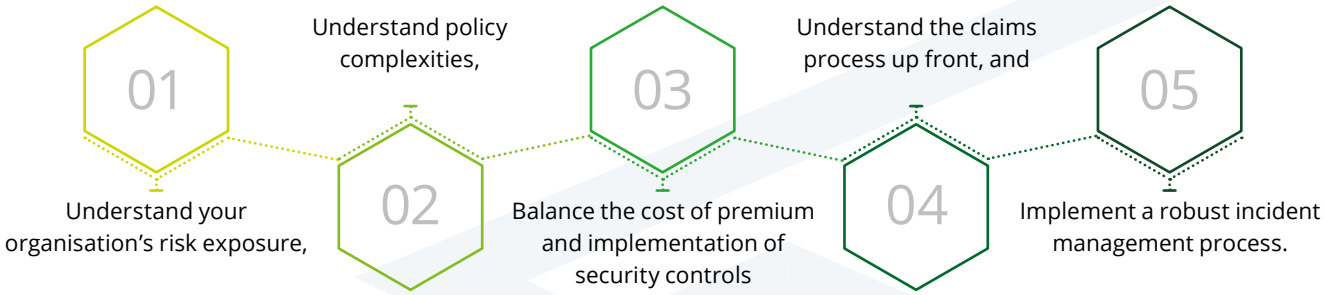
Cover includes

- Costs associated to investigate and resolve information security breaches.
- Allow organisations to manage their risk through risk transfer.
- Enable policies to be structured to protect the most important areas of an organization, whether it is social media, cloud computing, or third party management.

Cover excludes

- Protection from reputational risk, i.e., the damage done to an organisation's brand due to a cyber-incident cannot be repaired as easily or transferred to an insurance carrier
- Insurance, whether cyber or otherwise, provides the organisation with the opportunity to transfer, not remove the risk
- Replacement for an information security programme within an organization

When selecting a cyber-insurance policy, here are some critical considerations that an organisation must make



Allow us to manage your Cyber Risk

At Deloitte, we offer a range of services throughout the cyber insurance lifecycle that help organisations to manage their cyber risks appropriately.

Identify Cyber Risk Exposures:

- Determine the cyber risk exposures and potential financial affects.
- Determine the level of mitigation required before transferring the risks.

Assess Cyber Insurance Options:

- Obtain inputs from various insurance providers for the coverage required.
- Compare various cyber insurance options available and provide recommendations.

Remediation Options and Roadmap:

- Identify uninsurable risks and assist with mitigation.
- Develop a roadmap to mature cyber security programme.

Incident Management Process Implementation:

- Develop and implement a streamlined process for incident management and claims filing.

Contacts

Rohit Mahajan
President, Risk Advisory
rmahajan@deloitte.com

Gaurav Shukla
Partner
shuklagaurav@deloitte.com

Anand Venkatraman
Partner
anandv@deloitte.com

Deloitte.