Cyber Insurance: A Crucial Element In Corporate Risk Management Strategy
India has witnessed a significant 37% increase in cyberattacks.

Executive Summary

Experts consider cyberattacks to be inevitable in a broad sense. The question now is not ‘if’ they will happen, but ‘when.’ Notably, it has never been so relevant than it is today, in a Post-COVID-19 era. For instance, India has witnessed a significant 37% increase in cyberattacks in the first three months of the year 2020. Recent attacks have shown that security lapses can devastate organizations, considering the magnitude of the losses.

Cyberattacks erode brand reputation, cause substantial financial damages, and lead to loss of customer trust. Although it is impossible to be completely secure, organizations can develop a robust cyber risk management plan to implement efficient measures for detection, prevention, and response to threats. These measures can reduce risks to an acceptable level.

Cyber insurance has emerged as an essential part of an enterprise’s cyber risk management plan and protects the organization’s information assets by transferring cyber risks to insurance providers.
Are You Considering Adopting Cyber Insurance?  
Have A Look At The Economic Costs Of Cybercrime

A look at the most massive breaches of the past decade reveals that the attacks have cost enterprises several hundred million dollars in financial damages.

According to a recent report from IBM and the Ponemon Institute, the worldwide average cost of a data breach in 2019 was $3,92 million. We can expect it to grow in 2020 due to recent fast-paced digitization due to COVID-19.

According to a new study by IBM, the average cost of a data breach in India alone has reached to Rs 12.8 crore.

These costs may include investigation costs, credit monitoring costs, the cost for remedial activities, paid ransom, notifying affected customers, PR and reputation management, legal fees, settlements, and regulatory fines.

Fast-forward 2020: What's New In Cyberspace?

COVID-19 has changed the way businesses used to operate. Growth in the number of virtual workers and increased digitization has also elevated the number of cyberattacks taking place. As per a recent Verizon report, 45% of the data breaches were due to hacking, but surprisingly 22% were casual errors:
This phenomenon paints a grim picture and also a warning for organizations to be prepared for both external or internal threats, intentional or accidental information damages.

**Cyber Insurance Defined**

Cyber insurance is an insurance product that organizations use to protect themselves from digital risks and risks related to their computing environment, IT activities, and infrastructure in general.

The losses covered by cyber insurance fall into two broad categories. First-party losses are direct losses that fall on the organization that suffered a breach. Third-party damages are the costs that third parties, such as customers and partners, vendors, and contractors incur due to cyber incidents.
So How Does It Benefit Having A Cyber Insurance?

The following are the significant benefits cyber insurance can offer to any organization:

- **Insurance Imparts Financial Resilience**
  
  Organizations that suffer breaches can mitigate the insured share of the loss and recoup out-of-pocket losses.

- **Strengthened Regulator’s Trust**
  
  The US SEC requires organizations to disclose financial positions on cyber risk and insurance. Organizations that go through cyber insurance placement processes create a record of actively managing cyber threats.

- **Better Contracts Alignment**
  
  Organizations dealing with business operations that require accessing, processing, and storing of PII or ‘Personally Identifiable Information’ and other protected information assets can streamline contracts with the third parties concerned. The third parties get assurance concerning protection in case of an incident.

- **Enhanced Customer/Client Trust**
  
  Your customers are more likely to trust your enterprise if they know you are serious and care about protecting their confidential and sensitive financial or personal information, and even in case of an incident, the enterprise has enough financial support to resume business operations quickly.
What Kind Of Coverage Does Cyber Insurance Provide?

Every cyber insurance provider has its own terms and conditions, types of covers (what they cover, and what they do not, how much they cover, etc.) and hence individuals and organizations are advised to take extreme care of and do their own due diligence before selecting a cyber insurance provider or a coverage type that suits their unique needs. Given below is a partial list of covered incidents organizations may consider in the coverage they are planning for:

01 Legal Costs
Legal costs can be crippling, especially for SMEs and Startups, and lawsuits against organizations add to losses. However, large business organizations, on the other hand, can face lawsuits.

02 Regulatory Penalties
Violations of regulations concerning data confidentiality and integrity, or user data privacy such as HIPAA, GDPR, etc. can lead to hefty fines.

03 Investigations
Forensic costs are related to the analysis of an attack, and experts must carry out forensic examinations.

04 Notification Costs
Breached organizations are often required by law to inform clients, suppliers, and partners who have been affected. Such activities help in brand reputation management.

05 PR Costs
Larger breaches may need extensive communications with the press and other organizations to safeguard the reputation.

06 Credit Monitoring Costs
Credit monitoring is often required after a data breach and helps protect organizations from financial fraud and identity theft.

07 Breach Coaching
Breach coaches are high-level response coordinators who work with experts to identify and isolate affected data, notify clients, hire forensic investigators, and manage PR. They are first responders and conduct triage.
What Incidents Are Not Covered By Cyber Insurance?

Organizations should also be aware of the incidents that may not be covered by all or specific cyber insurance providers and thus take a cognitive decision before selecting one. These incidents may include:

- **Intellectual Property Theft**
- **Remediation of Breaches**
- **Protection from Reputational Risks**

Cyber insurance cannot guarantee the removal of risks; it only transfers risks. Also, cyber insurance is not a replacement for a robust infosec program that includes reliable security controls. Having a robust information security program is, in fact, a pre-requisite for purchasing cyber insurance. To properly understand what incidents are covered, employees concerned, such as CISOs must thoroughly read the policy.
Best Practices When Selecting Cyber Insurance

Some best practices to be followed when placing a cyber insurance policy are-

1. **Undergo a Cyber Insurance Placement Process** - Insurance is not mandatory for every organization. Still, all organizations should evaluate and document the steps that led to the purchase or decline of the insurance. All organizations should also go through a cyber insurance placement process to access their risk profile and tolerance.

2. **Employ the Services of an Experienced Broker** - Organizations must employ brokers that are cyber-savvy, knowledgeable about cyber risks, and understand how insurance organizations currently assess different risk levels.

3. **Go Beyond the Bare Minimum** - As an internal exercise, organizations should go beyond just the questions in an application form and demonstrate their ability to minimize risk and security posture. They should provide underwriters with a clear picture of the cyber-risks faced by them.

4. **Aim for ‘Fair’ Prices rather than ‘Best’ Prices** - The cyber insurance market lacks unity and maturity, and thus getting the most useful coverage at a fair price should be a priority.

5. **Engage Cyber Security Experts** - Third-party consultants or security organizations working in tandem with brokers can assist in navigating the process. The assistance of legal counsel experienced in cyber insurance should also be taken.

![How did you determine the level of cyber risk to your company?](chart1)

**Figure 2**: How companies determined their cyber risk
Perform A Security Assessment Before Filling In The Application

Generally, an independent third-party assessment should be considered for an unbiased evaluation of your organization's security posture. Security Assessments can help organizations in three ways:

1. Revealing current vulnerabilities and methods of improving the organization's security stance.
2. Helping both the broker and underwriter by documenting the current state of response readiness.
3. Estimating what level of coverage is required and what the sub-limits and limits should be.

Final Words

Cybersecurity in an organization is everyone's responsibility. However, no individual, organization, cybersecurity framework, or technology solution can guarantee 100% protection from cybercrime or cyberattacks. Even the best-planned internal control measures can fail in the face of zero-day threats or fraudulent schemes, imagine a disgruntled employee or untrusted contractor in your enterprise environment.

Cyber insurance thus needs to be a vital element of every organization's risk management strategy. The decision to purchase or decline coverage should be documented and should include all critical stakeholders, including Risk Management, CFO, CEO, CISO, the Legal Team, and the board. Although more organizations have been inclining towards purchasing cyber insurance, no policy fits all enterprises. Organizations should secure coverage that will address the unique cyber risks they face and the business environment they operate in.
References

https://www2.deloitte.com/content/dam/Deloitte/cy/Documents/risk/CY_Risk_Cyberinsurance_Noexp.PDF
https://www.ii.org/sites/default/files/docs/pdf/cyber_risk_wp_103017.PDF
https://amp.insurancejournal.com/magazines/mag-features/2020/04/20/565224.htm