KPMG

Cyber Insurance Advisory

Risk matters

home.kpmg/jm

Setting the context

Cyber-attacks are on the rise. Hackers are increasingly looking to take advantage of security vulnerabilities to steal valuable customer data. For organisations, the impact of these attacks goes far beyond just data loss, from significant PR fallout and loss of customer trust at one end to regulatory penalties at the other.

What is cyber insurance?

Traditional insurance products provide coverage over commercial general liability, errors and omissions (E&O), directors and officers (D&O) etc. The insurance cover provided by these products is often inadequate for risks emanating from cyber-attacks.

Cyber insurance policy is an insurance policy that is provided to organisations in order to protect them from losses arising due to cyber-attacks, which includes, but not limited to the following:

- Forensic investigation costs
- Administrative fines
- Cyber extortion expenses
- Breach notification costs
- Legal expenses.

Cyber insurance drivers for organisations

Increase in the cost of data breaches

The average total cost of a data breach is USD 3.86 million[1]

Evolving regulatory landscape

One of the major drivers for cyber insurance has been regulations. Regulations such as the General Data Protection Regulation (GDPR) can potentially impose heavy fines and penalties on organisations in case of non-compliance

Third party risks

In the light of major cyber incidents globally, organisations have been strengthening their third party risk posture and including cyber insurance as part of vendor contracts

Number of organisations (in %) recovering cyber losses through cyber insurance policy[1]

- 51% for legal/ consulting services
- 30% for regulatory fines
- 29% for recovery technology
- 10% for ransomware

1. Cost of a Data Breach Report, Ponemon Institute, 2020

The cyber insurance dilemma

While most insurance products are based on decades of aggregated and actuarial data, assessing cyber risks and pricing cyber insurance products is difficult because of the evolving cyber landscape and lack of historical data for actuaries to work with. In the absence of an appropriate analysis of the cyber risk exposure, organisations can either end up with insufficient insurance cover or paying up additional premium for a larger cover which may not be required.

What should organisations do?

Understand your cyber risk posture

Organisations should understand their cyber risk posture by conducting cyber risk assessments covering their scale of operations and business portfolios across geographies, regulatory and statutory obligations, involvement of third parties, cyber incident history and practices followed for information security, data privacy and business resilience.

Identify the right policy

Once you know the cyber cover required it is important to identify the right insurance policy with regard to inclusions, exclusions, first and third party cover etc.

Periodically re-evaluate

In a dynamically evolving landscape, cyber risks are constantly increasing hence it is imperative to periodically re-evaluate the cyber posture of your organisation and accordingly revisit the cyber insurance policy.

How can we help?

In order to assist organisations and insurance agencies, an in-house tool has been developed, which takes a quantitative approach to assess, mitigate and transfer cyber risks. In order to execute our cyber insurance advisory services, we have formulated a three phased approach which includes:

Cyber risk assessment:

- Review the company profile, IT landscape, cyber incident history
- Assess the cyber risk posture and identify remediation measures across the following domains:
  - Leadership and governance
  - Legal and regulatory compliance
  - Information security and privacy
  - Risk management
  - Vendor management
  - Incident and breach management

Cyber insurance modelling:

- A fully automated, algorithm based statistical model to quantify cyber risk exposure
- Use of historical loss data (depending on availability), IT landscape and cyber risk maturity for customised outputs
- Optimised cyber insurance plan by using Monte-Carlo simulations, with over one million scenarios
- Feedback to Enterprise Risk Management (ERM) committees by providing inputs to cyber risk KPIs for relevant decision making and governance.

Monitoring and reporting:

- Periodic review of changing cyber risk profile and quantifying cyber risks posed to entity
- Analysis of breach of risk appetite
- Detailed report on assessment

Key takeaways

- Independent reporting on current cyber security risk posture
- Remediation controls and implementation roadmap for identified cyber security risks
- Cost-benefit analysis of control implementation expenses versus insurance cover
- Structuring a suitable cyber insurance program with an optimal cover
- Comprehensive risk-based assessment to estimate insurance premium
- Cyber insurance policy comparative analysis
- Estimation of risk appetite and retained losses at an appropriate level of confidence
- Cyber insurance product pricing for Insurance providers

KPMG in CARICOM contacts:

Raymond Campbell
Partner and Head
Advisory
KPMG in Jamaica
T: +1 876 922 6640
E: raymondcampbell@kpmg.com.jm

Dushyant Sookram
Managing Partner
Head Advisory
KPMG in Trinidad and Tobago
T: +1 868 612 5764
E: dsookram@kpmg.co.tt

Christopher Brome
Partner
Head Advisory
KPMG in Barbados and the Eastern Caribbean
T: +1 246 434 3900
E: cbrome@kpmg.bb

home.kpmg/jm

Follow us on: socialmedia