Cyber Security Insurance Policy

The Cyber Security policy indemnifies an Insured for third party claims, regulatory fines and penalties; and first party costs and expenses incurred after an attack or an unauthorized access/ transmission /compromise on the company's Information security network and systems.

Who should buy Cyber Insurance Policy?
Organizations should be concerned about cyber risk if they:

- Gather, maintain, disseminate or store private information
- Have a high degree of dependency on electronic processes or computer networks
- Engage vendors, independent contractors or additional service providers
- Are subject to regulatory statutes
- Are required to comply with PCI Security Standards/Plastic Card Security statutes
- Are concerned about intentional acts by rogue employees
- Are a public company subject to the SEC Cyber Disclosure Guidance of 2011

The cyber Insurance policy offers a range of covers under one insurance program. The two main areas of coverage are with respect to

(1) Privacy breach and related liability exposure

(2) Various costs which cause a direct financial impact on the affected business

Please find below a table showing the cyber events that the policy covers and the corresponding first party and third party losses that would be paid under the policy

CYBER EVENTS	INSURED LOSSES - First Party directly paid or incurred by the Insured	INSURED LOSSES - Liability arising from a Claim or Investigation targeting the Insured
Data Breach	• Emergency Response Costs • Event Management Costs • Notification Costs • Monitoring Costs • Recovery Costs	• Damages • Regulatory Fines and Penalties • Defence Costs • Investigation Costs
Cyber Attack	• Emergency Response Costs • Event Management Costs • Diverted Funds • Recovery Costs	• Damages • Defence Costs • Investigation Costs
Human Error	• Emergency Response Costs • Event Management Costs • Recovery Costs	• Damages • Defence Costs • Investigation Costs
Insured's Systems Disruption	• BI Loss	• N/A
PCI Non-compliance	• Emergency Response Costs • Event Management Costs	• Damages • PCI Penalties • Defence Costs • Investigation Costs
Electronic Media Claim	• Emergency Response Costs	• Damages

	• Event Management Costs	• Defence Costs
E-threat	• E-threat Response Costs	• Damages • Defence Costs

Data Breach: Any of the following if actually or allegedly committed or permitted by an Insured Entity or any other entity holding or processing Protected Data on behalf of the Insured Entity:

(a) The inadvertent loss, destruction or alteration of, or
(b) The unauthorised disclosure or dissemination of or access to,

Protected Data lawfully collected and held by or on behalf on the Insured Entity, including due to the negligent (but not reckless or deliberate) loss of documents, hardware or any other media containing access or security information.

Cyber Attack: The fraudulent, malicious or dishonest: causing or use of a Security Breach, or disruption or overload of the Insured's Systems by a Third Party for any purpose.

Human Error: A Security Breach inadvertently caused or contributed by negligent acts or errors in the active maintenance, operation, programming or update of the Insured's Systems by or on behalf of the Insured Entity

Insured's System Disruption: The unavoidable interruption, unavailability or disruption, in whole or in part, of the Insured's Systems as the sole and direct result of a Cyber Attack, Human Error, or a systems shutdown ordered by a competent civil authority or recommended by the IT Response Team in response to a Cyber Attack.

PCI Non Compliance: Any actual or alleged non-compliance of the Insured Entity with the Payment Card Industry Data Security Standards

Electronic Media Claim: Any Claim made against the Insured Entity by a Third Party arising directly and exclusively from: libel, slander or any other reputational damage, or breach of any intellectual property right, right of publicity or privacy right, alleged to have resulted from the content of, or deep-linking or framing within, a public webpage or e-mailing designed and / or sent for the business of the Insured Entity.

E-Threat: A verifiable threat made specifically to the Insured Entity by any means (including ransomware) to commit a Cyber Attack, or not to put an end to an existing Cyber Attack unless certain conditions (including payments) are met.

Exclusions:

1. Known Matters
2. Infrastructure Failures
3. Deliberate or Reckless Conduct
4. Insolvency
5. Bodily Injury and Physical Damage
6. War and Terrorism
7. Patens

Please read the policy wording for complete coverage, terms and conditions