

Cyber Insurance Checklist

This template is intended as a starting point for evaluating coverage. Based on your organization's size, business sectors, and geographic locations you operate in, your needs may vary.

Protections and Policies	
<input type="checkbox"/>	The coverage for the loss due to operational issues by the employees.
<input type="checkbox"/>	Cyber extortion reimbursement costs including a credible threat to introduce malicious code; pharm and phish customer systems; or to corrupt, damage, or destroy systems.
<input type="checkbox"/>	Electronic media peril broadly defined to include infringement of domain name, copy right, trade names, logo, and service mark on internet or intranet site.
<input type="checkbox"/>	Interruption expenses include costs associated with rented/leased equipment, use of third-party services, staff expenses, or labor costs directly resulting from a covered loss.
<input type="checkbox"/>	Personally identifiable information (PII) broadly defined to include an individual's name in combination with social security number, driver's license number, account number, credit or debit card, or any non-personal information as defined in any privacy regulation.
<input type="checkbox"/>	The policy should be made under the knowledge provision of Board of Directors, President, Executive Officer, Chairman, Chief Information Officer, Chief Technology Officer, Risk Manager, or General Counsel.
<input type="checkbox"/>	The policy should have the coverage for damages to third parties caused by a breach of network security.
<input type="checkbox"/>	It must have coverage to comply with an alleged breach notice order issued by a regulatory agency.
<input type="checkbox"/>	The coverage should also include expenses consumer protection laws such as the Fair Credit Reporting Act (FCRA), the California Consumer Credit Reporting Agencies Act (CCCRAA), and the EU Data Protection Act.
<input type="checkbox"/>	The policy should cover the reputation cost it takes to repair public relations as a result of a data breach.
<input type="checkbox"/>	The coverage should also include the damages made by cyber extortion, cyber terrorism, and ransomware attack(s).
<input type="checkbox"/>	The coverage should also include financial losses due to online fraudulent fund transactions through fake websites.

<input type="checkbox"/>	The policy covering customer breach notice expense such as reimburses for costs to notify and remediation costs including but not limited to credit monitoring.
<input type="checkbox"/>	The coverage should also include the damage made by the disgruntled employee(s).
<input type="checkbox"/>	The coverage should include the expenses spent on forensic examination, legal proceedings, remediation, and other costs. Coverage for contractual liabilities including PCI-DSS costs.
<input type="checkbox"/>	The policy should have a coverage for severe damages to the infrastructure.
<input type="checkbox"/>	The policy should contain the coverage of loss of revenue and business reputation during an incident.
<input type="checkbox"/>	The coverage should include the expenses spent to recover the lost or corrupted data caused by cyber-attack.
<input type="checkbox"/>	The coverage should include the expenses for replacing the affected devices due to cyber-attack.

Cyber Insurance Claim Covers	
<input type="checkbox"/>	Network and connected devices
<input type="checkbox"/>	Hardware and software assets, including applications, operating systems, and security solutions
<input type="checkbox"/>	Staff and other human resources
<input type="checkbox"/>	Reasonable response time for data breach incidents, including recovery and response planning
<input type="checkbox"/>	Digital assets, including stolen and lost data
<input type="checkbox"/>	Legal and compliant settlements, as well as governmental fines
<input type="checkbox"/>	Expenses for IR, recovery, and forensics
<input type="checkbox"/>	Protection from terrorism and cyber extortion