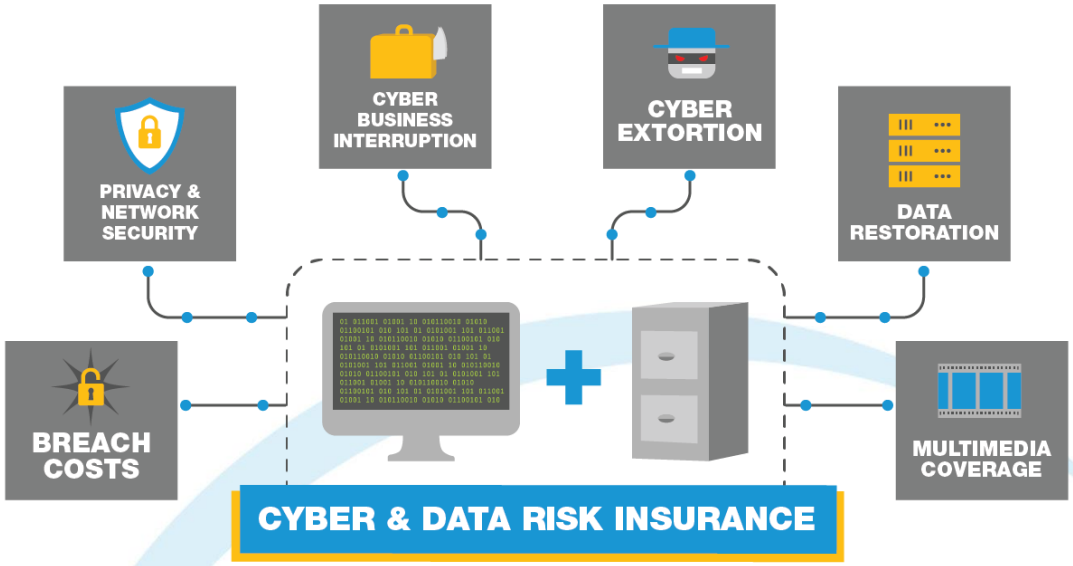
Worldwide Facilities®, LLC

Experience a World of Difference

wwfi.com

CA License #0414108



What Is Cyber & Data Risks Insurance?

Cyber & Data Risks policies are designed to address several issues through various coverage parts or modules (if elected). Though the coverage component titles may vary among different insurance carriers, the general scope can be defined as follows:

BREACH COSTS

Coverage for costs associated with responding to a breach, such as forensic costs to confirm and identify the breach, costs to notify affected individuals, identity protection services including costs to staff a call center for redemption of monitoring offers, and crisis management/public relations costs.

PRIVACY & NETWORK SECURITY

Covers costs to defend and resolve claims regarding the handling of personally identifiable or confidential corporate information. Covers negligence, violation of privacy or consumer protection laws, and regulatory investigations. Many forms also cover breach of contract issues relating to the security of sensitive information or payment card data. Coverage also extends to the failure of your network security, including the negligent

transmission of a virus and the inadvertent participation in a Distributed Denial of Service (DDoS) attack against a third party.

CYBER BUSINESS INTERRUPTION

Covers network-dependent business income loss due to malicious network interruptions. Some coverage may also extend a sub-limit for dependent network outages, such as your cloud provider.

CYBER EXTORTION

Covers the response costs and financial payments associated with network-based ransom demands. These issues may proliferate through physical breaches, or the extortion-based subset of malware referred to as ransomware.

DATA RESTORATION

Covers costs to recreate or repair data, systems, or programs damaged or destroyed in a malicious attack.

MULTIMEDIA COVERAGE

Costs to defend and resolve claims related to advertising content, such as defamation or copyright/trademark infringement.

Cyber & Data risks coverage can typically be purchased as a package or on an à la carte basis, with the Breach Costs & Privacy/Network Security components serving as the foundation for the policy.

Most cyber policies extend coverage to online media operations only, but offline / print media coverage may be available via endorsement.

Why Buy Cyber & Data Risks Insurance?

VENDORS, VENDORS, VENDORS

You've lost a laptop, mailed financial records to the wrong recipient, or noticed unauthorized activity on your network. What do you do? Who do you call?

Upon a breach, you will need one or more of the following components:

- Forensics analysis to determine the size and scope of the issue.
- Legal consultation and drafting of notification letters to individuals.
- Mailing & Postage services for notifications to affected individuals.
- Credit/Identity monitoring services if Personally Identifiable.
- Information has been compromised.
- Operational call-center to field identity monitoring redemptions.
- Public relations & crisis management firms to manage the fallout.

A Cyber & Data Risks policy placed with a specialized insurer will guarantee your access (with negotiated rates) to the best in the business.

BOTTOM-LINE AND BOARD SEAT PROTECTION

Data breaches are an insurable risk. It is increasingly common to find board members being ousted due sub-par breach response execution. The world has come to understand that breaches are not always preventable, but poor breach responses are preventable.

LEGAL & REGULATORY REQUIREMENTS

Navigating 48 different data breach notification laws is difficult. Each may have a varying definition of what constitutes Personally Identifiable Information (PII). Responsibilities placed on companies through HIPAA, GLB, FACTA and the Payment Card Industry Data Security Standard can cost millions in the event of a breach.

PEOPLE

Despite evidence that no system is completely secure, some may feel that they have the best IT security on the planet. Even if this were true, you can never truly secure your employees. Mobile devices, inadvertent clicks, nefarious e-mails, and social engineering attempts keep you only a step away from disaster. Internal employees who become disgruntled can also create an extremely hazardous situation when they gain access to sensitive information or systems.

THE CLOUD

Cloud providers understand that they cannot indemnify everyone on the planet in the event of a breach. Your hosting contract most likely disclaims all liability from your provider. Further, your cloud deployments are also subject to vulnerabilities that are waiting to be exploited by no fault of your provider.

Payment Cards (Debit & Credit) – If you accept them, you have the liability.

Even if you outsource your point of sale system, payment processing, or other portion of the payment chain, you can still find yourself liable for PCI fines, penalties, and assessments in the event of a payment card breach. Most of the payment card breaches in the news did not result from a huge repository of stored payment card information being breached, rather those incidents occurred after malicious software was able to siphon off card data in real-time.

Many insurance policies in the marketplace inadequately address this exposure by either excluding/sub-limiting coverage, or only covering certain portions of the fallout. It is important to ensure all PCI Fines, Penalties and Assessments (card reissuance and fraud charges) are included in the scope of coverage.

There are four levels of PCI compliance, which include higher levels of security requirements based on higher volumes of payment card transactions.

Merchants that qualify as Level "4" can self-assess, while merchants that transact a higher volume of card data must contract with a Qualified Security Assessor and Approved Scanning Vendor, per the Payment Card Industry Data Security Standard (PCI-DSS)

Levels of compliance (Level 4 can optionally get a third-party validation or self-assess):

Merchant Level	Description
1	Any merchant—regardless of acceptance channel—processing over 6M Visa transactions per year. Any merchant that Visa, at its sole discretion, determines should meet the Level 1 merchant requirements to minimize risk to the Visa system.
2	Any merchant—regardless of acceptance channel—processing 1M–6M Visa transactions per year.
3	Any merchant processing 20,000 to 1M Visa e-commerce transactions per year.
4	Any merchant processing fewer than 20,000 Visa e-commerce transactions per year, and all other merchants—regardless of acceptance channel— processing up to 1M Visa transactions per year.

PCI LINKS

- PCI Self-Assessment
- PCI Security Standards Document Library
- You can qualify with the vendor what the vendor's capabilities are and what is required for validation, but you would generally engage a QSA (Qualified Security Assessor) when validating compliance and utilize the services of an ASV (Approved Scanning Vendor) for ongoing maintenance every 90 days:
    - Qualified Security Assessor (QSA)
    - Approved Scanning Vendors (ASV)

When Should You Contact Your Agent?

Navigating a breach response successfully can be imperative to the survival of your organization. To do this, you must ensure that your policy sits at the forefront of your breach response plan. This policy provides access to a wealth of knowledge, experienced vendors, and breach response firms that will help you drive your organization out of your breach nightmare. You should notify your agent immediately upon (*but not limited to)* any of the following scenarios occurring:

- Any incident occurs that may be considered a claim or ***notice of circumstance*** according to your policy. The definitions of claim or circumstance can vary from carrier to carrier, so it is best to keep your agent on notice when any information is lost or suspicious network activity is detected (including viruses/malware).
- Any time a device storing sensitive data is lost (including paper).
- Any time you are subject-to a network outage or loss of sensitive data. While not all outage scenarios are contemplated by cyber insurance policies, these circumstances should be reported early and often.
- Any time an ownership change is possible. Your policy may not respond to events occurring after a change in ownership or merger with another company. Your agent should confirm how to proceed with your underwriter.
- Any time your business operations drive a substantial increase in the Personally Identifiable Information stored/processed by your company. A new contract may bring on 50,000 new sensitive records. Situations like these may call for increased limits if you wish to adequately insure your exposure.

Don't let this happen to you!

Claims can be denied for late notice.

Get your carrier on notice and take advantage of the breach response services afforded to you.