THE CYBER SAVVY BROKER'S GUIDE

Demystifying Cyber Coverage

The Opportunity for Brokers

The global cyber insurance market is one of the fastest-growing commercial insurance segments, estimated to reach $28B by the year 2028.[1] This is driven by the increasing realization that technology is the lifeblood of every business.

However, 64% of small businesses are not familiar with cyber insurance and only 17% currently have a policy.[2]

Digital risks are evolving as quickly, often hiding in plain sight as the flow of information accelerates and threatens the things we value most. Brokers have the opportunity to build a deeper, more strategic partnership with their clients as trusted cyber insurance advisors.

What Makes Cyber Coverage Unique?

Not all policies are created equal

Although cyber policies are structurally similar to traditional professional lines of insurance, the uniqueness of the cyber policy lies in the immediate expert attention dedicated to the insured towards identifying, preventing, and mitigating a cyber incident.

When partnering with a cyber insurance provider, brokers can seek unique coverage solutions that offer broad protection along with holistic risk management tools for their clients.

How is a Cyber Policy Structured?

See the full list of Cyber Coverages designed for digital risks

First Party

Coverage for your client

Out-of-pocket expenses an organization incurs to recover from a loss, such as:

- Breach Response
- Business Interruption
- Cyber Extortion

Broker Opportunity
Help your clients understand the value behind the policy and how quickly costs can add up.

Third Party

Everyone outside of your client's organization

Any resulting liability or third party action as a result of a cyber incident, such as:

- Network & Information Security Liability
- Regulatory Defense & Penalties
- Technology and Media Liability

Broker Opportunity
Help your clients consider the potential liability and resulting expenses of a cyber incident.

1. Vantage Market Research 2. AdvisorSmith

Continued →

How to Future-Proof Cyber Coverage

A comprehensive cyber policy includes coverage for emerging digital risk exposures, including:

Bodily Injury and Property Damage (BIPD)
The liability and first party costs to a third party when a security failure results in physical damage or injury to anyone outside the organization.

- Plus first party costs when a security failure leads to property damage which then results in a covered loss (e.g., damage to industrial controls, etc).

Service Fraud
Financial loss incurred from the fraudulent use of business services, including cryptojacking.

Computer Replacement
Costs to restore or replace computer hardware if systems are permanently impacted by malware.

Reputational Loss
Includes net profit that would have been earned in the absence of a public negative media event.

Evaluating Cyber Policies

What brokers should look for when placing cyber coverage:

1. **Comprehensive Coverage**
   Broad, foundational coverage designed for cyber attacks such as ransomware, phishing, and funds transfer fraud (FTF)
2. **Favorable Coverage Features**
   Pay on behalf of language, breach response outside the limits, and $0 retention for breach response services
3. **Active Risk Management Solutions**
   Continuous monitoring and alerting for emerging threats and vulnerabilities with Coalition Control
4. **Dedicated Technical Support**
   Pre-Claim Assistance, In-house Claims and Incident Response forensic specialists who respond in minutes
5. **Limitations of exclusions and package policies**
   Be mindful of exclusions such as fraud and prior knowledge

Why Coalition

As the world's first Active Insurance company, Coalition combines comprehensive insurance and proactive cybersecurity tools designed to help businesses manage and mitigate cyber risks. Coalition policyholders experienced 50% fewer claims compared to organizations with passive cyber coverage.[3]

Get Active for your clients. Get started quoting with Coalition today.

3. Coalition 2022 Cyber Claims Report