

WHAT A CYBER POLICY SHOULD LOOK LIKE



WHAT SHOULD YOU LOOK FOR IN A CYBER POLICY?

- Access to a 24/7 breach hotline
- Incident response costs, such as computer forensic services, legal counsel and customer notification and call center services
- The cost of recovering or replacing lost or stolen data
- Income loss due to business interruption following a cyber incident
- Cybercrime—i.e. electronic funds transfer, extortion and fraud
- Third-party coverage, such as payments to consumers affected by a breach, litigation costs, and losses related to defamation and intellectual property rights infringement

CONSIDER WHETHER THE PROVIDER WILL...

- Defend you in a lawsuit or regulatory investigation (look for “duty to defend” wording)
- Provide coverage in excess of any other applicable insurance you have

FIRST-PARTY COVERAGE

First-party cyber coverage protects your data, including employee and customer information. This coverage typically includes your business’s costs related to:

- Legal counsel to determine your notification and regulatory obligations
- Recovery and replacement of lost or stolen data
- Customer notification and call center services
- Lost income due to business interruption
- Crisis management and public relations
- Cyber extortion and fraud
- Forensic services to investigate the breach
- Fees, fines, and penalties related to the cyber incident

THIRD-PARTY COVERAGE

Third-party cyber coverage generally protects you from liability if a third party brings claims against you. This coverage typically includes:

- Payments to consumers affected by the breach
- Claims and settlement expenses relating to disputes or lawsuits
- Losses related to defamation and copyright or trademark infringement
- Costs for litigation and responding to regulatory inquiries
- Other settlements, damages, and judgments
- Accounting costs

3 CYBER POLICY "TRAPS"

- Data re-creation vs data recovery
- Call back warranties
- Aggregate limits

Talk to us about not falling into these traps and ensuring you have the right coverage in place to help prevent, respond to and recover from cyberattacks.



About Insgroup

Insgroup was founded in 1978 in Houston, Texas, by a group of entrepreneurs committed to a shared vision to provide the security necessary for business owners and individuals to pursue their dreams. Over the next four decades and through changes in leadership and tremendous growth, our vision has remained unchanged. We have become one of the largest independent firms in Texas and one of the top 100 in the country, but we have stayed true to our roots.

Clients appreciate that we are not generalists, but a collection of experts. Today, Insgroup is comprised of 200 colleagues with expertise in Property & Casualty Brokerage, Employee Benefit Consulting, Private Risk Services, and Surety. We serve clients nationwide and partner with premier national, regional and specialty insurance carriers across the United States.

This material has been prepared for informational purposes only.

BRP Group, Inc. and its affiliates, do not provide tax, legal or accounting advice. Please consult with your own tax, legal or accounting professionals before engaging in any transaction.