RISK strategies

CYBER LIABILITY

Cyber criminals are targeting businesses of all sizes — from startups to Fortune 500.

If you're large enough to have a cybersecurity team, you also have more digital assets to protect. This means more potential entry points for attackers to compromise your data and operations.

Smaller businesses often have no security team. Threat actors may assume you're not tightly monitoring cybersecurity.

We help organizations of all sizes protect against cyber risk, so you can concentrate on your core mission.

QUESTIONS TO ASK

Today, insurers want to see a cyber threat assessment before underwriting a new cyber liability policy or calculating renewal rates. How do you currently conduct these assessments?

Underwriters also probe topics like these:

- Can your employees accurately distinguish between a legitimate email and a potential phishing email?
- How are you protecting endpoint devices not owned by IT? If your facilities team handles your smart thermostats, are they monitoring the cybersecurity of that equipment?
- Do you use third-party software products to run your business? Are you observing their cybersecurity or relying on it without oversight?
- Have any of your third-party vendors (payroll, credit card processing, order fulfillment, cloud, etc.) experienced a breach in the past 12 months?

Your organization is responsible for protecting your customers' data. That's true even if you outsource business activities to a third party.

> **If a cyberattack locked you out of your computer systems, what steps would you take to recover?**

SOLUTIONS & CAPABILITIES

As the types and frequency of cybercrime increase, how can you safeguard your organization's data, reputation, and bottom line? Having the right risk management protocols and insurance coverage can reduce the financial impact and recovery time after a cyberattack.

Risk Strategies specialists...

- Maintain strong relationships with key insurers to bring you the most comprehensive coverage at the best price — cyber liability, technology errors and omissions, professional liability, media liability
- Offer complimentary external infrastructure vulnerability scans to identify threats
- Analyze claims trends to guide cybersecurity risk management planning
- Perform loss modeling and limit benchmarking to inform coverage decisions
- Create risk mitigation strategies to deter cyberattacks and lessen damage if a breach occurs
- Facilitate tabletop exercises, employee training, and incident response planning to prepare your team for any cyber event
- Provide access to trusted vendors who can help with penetration testing, endpoint detection, and other specialty cybersecurity services to protect your digital assets

Clients get a dedicated cyber risk response and claims advocacy team, including in-house counsel. We help you navigate the claim process, so you receive the correct settlement amount under your policy.

You can reach our team by email or phone 24/7 to report a data security incident at any time of day or night, including weekends and holidays.

WHY RISK STRATEGIES?

The cyber threat landscape grows more complex by the day. Risk Strategies equips you to assess, mitigate, and respond.

We work closely with you to improve your risk profile, so insurance underwriters see your commitment to cybersecurity. Our specialists keep you up to date on emerging risks, evolving best practices, regulatory changes, and what to expect at renewal time so you can plan.

Let's Talk.
cyber@risk-strategies.com
riskstrategies.com

Risk Strategies | Risk management. Insurance and reinsurance placement. 30 specialty practices. Access to all major insurance markets. 9th largest privately held U.S. brokerage.