

Cyber Insurance Checklist

Educating Yourself: How to Stay Current in Cyber

- Read up on the latest news: Where to Start? [Here's How to Stay Current on Cyber Security News](#)
- Identify your specific risk: [Cyber Exposure: What's the Real Cost?](#)

Vetting the Insurer: Testing Their Abilities and Competence.

- What is the carrier's background and level of experience (specifically the claims team)?
- Does the carrier offer superior customer service?

Reviewing Coverages: Finding the Right Policy

- What is the crime sub-limit? Does this include social engineering?
- Does the policy offer funds coverages for:
 - [Ransomware](#): Do they offer a reimbursement policy? Or do they pay the loss directly?
 - Bricking: For any technological devices that are rendered useless due to an attack.
 - Full limits for PCI fines and assessments
- Are bodily injury or property damage coverages offered?
- Does the business interruption coverage extend to dependent business interruptions and system failure?
Do any specific exclusions apply?

Risk Management: Additional Services to Prevent Cyber Attacks.

- What risk management services are offered?
- Is proactive system monitoring included?
- Are scan reports completed regularly to ensure all software is up-to-date?