A guide to cyber insurance for modern businesses.

Cybercrime isn't just a big business problem — today's small businesses are growing targets of online attacks. In fact, research shows small businesses are three times more likely to be targeted by cybercriminals than larger companies. With recovery costs on the rise and customer trust on the line, the impact can be devastating. That's why cyber insurance for businesses has become essential in today's digital-first world. Learn why it matters and what cyber insurance can do.

Why cyber insurance matters

1. **Small businesses are growing targets.** Hackers often assume smaller businesses have less protection and weaker defenses. Because of this, many will target small businesses over larger corporations.

2. **Data breaches are costly.** Beyond immediate expenses like investigating the crime, breaches can lead to legal fees and regulatory fines. Cyber insurance helps cover these costs.

3. **Downtime is expensive.** The time and resources spent resolving a data breach can be significant. Cyber insurance reduces the financial impact of lost revenue and operational disruption, helping your business recover faster and get back to serving customers.

4. **Insurance protects your reputation.** If you experience a hack or data breach, customer information could be at risk. Cyber insurance can help cover the cost of notifying affected parties, providing credit monitoring, and managing legal or PR responses. It shows customers you're responsible and prepared.

5. **It offers peace of mind.** Business owners have enough to worry about on a day-to-day basis. Cyber insurance shields you from potentially devastating digital threats, so you can focus on growing your business instead of fearing an upcoming attack.

How to build a strong cyber protection plan

1. **Get cyber insurance.** It's the most important first step. A local, independent agent can help you choose cyber coverage that fits your business and protects against today's digital risks.
2. **Know your risks.** Two of the biggest mistakes small businesses make are failing to identify a potential threat and underestimating the severity of a known potential threat. Stay ahead of cybercrime by identifying your key digital risks.
3. **Educate your team.** Employees are often the first line of defense against scams. Train your team to recognize phishing emails, suspicious links, and other common threats.
4. **Use strong authentication.** Require multi-factor authentication when logging in and update passwords routinely, especially after team members leave your company.
5. **Update systems regularly.** Install software updates as soon as they're suggested and patch problems promptly. You don't want a vulnerability to sit for too long and leave you even more exposed.

Every business faces cyber risks, but you don't have to face them alone. Talk to a local, independent agent about added protection for your business today.