FAQ

WHAT IS CYBER INSURANCE?

When a breach occurs, cyber insurance covers the range of expenses that arise. These include identifying and solving the breach, recovering data, customer notifications, PR costs, possible credit monitoring expenses, legal expenses, potential fines from compliance regulators, extortion costs from ransomware, and general business interruption.

DO HACKERS REALLY BOTHER WITH ATTACKING SMALL BUSINESSES?

Yes. Hackers use technology to scan the internet for businesses with weak defenses regardless of the size of the business. A recent Verizon report notes that 43% of all cyber attacks are against small businesses. Worse, 63% of small businesses had experienced a breach in the last 12 months. Any business with a computer and an internet connection is at risk - even if you don't sell anything on your website.

WHAT'S COVERED?

First-party coverage – Intends to cover damages a business suffers because of a cyber breach. This can include things like investigative services, business interruption coverage and data recovery.

Third-party coverage – Intends to cover damages if a business' customers or partners are affected by a cyber attack. This can include legal fees, settlement costs, security failures and media liabilities.

Cyber crime — Intends to cover damage due to any type of illegal activity that occurs using digital means. Examples of cybercrime are extortion/ransomware, phishing, social engineering, and wire transfer fraud.

DOESN'T MY CURRENT BUSINESS INSURANCE INCLUDE CYBER ATTACKS?

Many general business protection policies only partially cover damage from cyber events, *if at all.* As mentioned above, cyber coverage protects against the vast array of possible damages, expenses, and lost business that can occur from a cyber attack.

WHAT SHOULD I CONSIDER WHEN CHOOSING BETWEEN PURCHASING A STAND-ALONE CYBER POLICY VS. ADDING AN ENDORSEMENT TO AN EXISTING POLICY?

To be fully protected, ensure you have all coverages – first-party, third-party, and cyber crime. Further, since some cyber events can result in large expenses, confirm you have adequate sublimits for each of three above coverages.

WHY DO I NEED A "BREACH COACH"?

If your company gets hacked, you will need a breach coach to get your business back up and running fast. When a breach occurs, you need to assess and contain the damage, notify affected parties (e.g. customers and vendors), evaluate and act on the legal ramifications from agitated customers to regulatory bodies, and more. A breach coach will quickly assemble the right response team to deal with these issues. Without an expert it all falls on you, costing you time and money while adversely affecting your business. Fortunately, most insurance companies now provide a breach coach as part of a greater suite of services when you purchase stand-alone cyber insurance coverage.

DO SMALL BUSINESSES NEED CYBER INSURANCE IF THEY PRACTICE GOOD CYBER HYGIENE?

Being properly protected definitely helps. However, there is no way to fully protect against new threats. Hackers are always adapting to overcome cyber defenses with new versions of current threats or creating brand new methods of attacking businesses. Human error can also be a factor. Easy-to-hack passwords, phishing emails, or even a lost laptop also present potential entry points for a cyber criminal. Additionally, a third-party vendor could be attacked, impacting your ability to do business and exposing your data. Even if you use a third-party vendor for business services, as the data owner you may be legally responsible. A thorough cyber insurance policy is part of your overall risk management plan to ensure your business runs smoothly.

* All of the above is general information which may vary based on context. Please consult the quote or ask an agent/broker for precise definitions and details.