Why Cyber Insurance Matters

Most businesses have a firm grasp on the physical assets and tangible risks they need to manage. But when it comes to virtual assets they need to protect – like financial information or other data – the overwhelming majority of businesses have a dangerous blind spot. Luckily, with a quick audit and some smart planning, you can make sure your business is protected, even in this fast-evolving digital economy.

Brought to you by

MANRY | HESTON

Understanding Cyber Risk

It's no secret-data drives our world and we're all connected through technology. The power of all this connectivity is amazing, but it also leaves us vulnerable to a cyberattack or data breach. These vulnerabilities and weaknesses can seem vague, so let's put some hard definitions to work to frame the real risk.

What is data risk?

PII: *Personally Identifiable Information*

Think of this as the numbers that identify us to government, financial and medical institutions. Social security and driver's license numbers, bank account information, online account usernames and passwords, medical and health insurance information – they're all keys that can unlock a wealth of personal data.

PHI: *Protected Health Information*

This covers information specifically relating to personal health – both medical histories and the provision and payment of healthcare that can be used to identify anyone who's ever seen a doctor or filled a prescription.

PCI: *Payment Card Information*

This is the specific information we carry in our wallets every day – the credit, debit and ATM numbers that unlock our financial accounts.

Why do cyber criminals steal PII?

It's pretty simple – PII is incredibly valuable. Unlike stealing a fixed asset like cash or jewelry, PII can be used to access ill-gotten gains or to even generate an ongoing stream of ongoing illicit revenue. Whether it's stealing employee Social Security numbers to establish new, fake lines of credit or extracting confidential information to sell on the black market, access to personal and confidential information can be easily monetized, in both the short run and over the long haul.

What Does Exposure Look Like?

The bottom line is businesses are liable in one way or the other for costs associated with a response to a data breach. These costs can be overwhelming – and confusing legislative requirements make it difficult for many businesses to overcome the fallout of a data breach without assistance.

Cyber insurance provides 1st and 3rd-party coverages for financial losses resulting from data breaches and other cyber events. Considering small businesses account for 58% of all data breaches, it's an essential coverage for any company that handles any form of personal information.

1st-Party Exposures

1st-Party Exposures are liabilities resulting from a breach but not requiring a lawsuit. Some key components include:

- **Computer forensics expenses** – used to identify the size and scope of breach or loss of information. These costs can vary greatly depending on breach size and complexity.
- **Notification of affected individuals** – rates can vary, but many carriers have negotiated rates that range from $1.25 to $5 per person notified.
- **Credit monitoring after loss of social security numbers** – widely available on the open market at upwards of $20 per year, but many carriers have negotiated rates in the range of $9-$13 per account per year
- **Regulatory fines or penalties** – these typically take two forms:
  - HIPAA: enforced by Health and Human Services and the Office of Civil Rights
  - Compensatory Awards
- **Public relations expenses** – the costs of managing perceptual fallout after a breach
- **Ransomware payments for cyber extortions**
- **Cyber crime** – social engineering and invoice manipulation

3rd-Party Exposures

3rd-Party Exposures are liabilities triggered after a lawsuit is filed by a third party. Some key components include:

- Class-action lawsuits
- Payment card reissuance expenses
- Payment card fraud expenses
- PCI fines and penalties
- Identity theft lawsuits
- Loss of 3rd-party intellectual property or confidential corporate information lawsuits
- Network disruption suits
- Bodily injury arising from lost data
- Mental distress due to exposure of privacy information
- Negligent transmission of a computer virus/worm or malicious code

What's the Right Coverage?

Navigating coverage needed to protect against the many exposures facing businesses today can be complicated. Some coverage categories to consider include:

Privacy Protection

Covers costs to defend and resolve claims regarding the handling of personally identifiable or confidential corporate information. Includes coverage for:

- Negligence, violation of privacy or consumer protection law, breach of contract and regulatory investigations.
- Issues resulting from the failure of network security, including the negligent transmission of a virus and the inadvertent participation in a DDoS attack against a third party.

Breach Costs

Covers costs associated with responding to a breach, such as forensic costs to confirm and identify the breach, costs to notify affected individuals, credit protection services including costs to staff a call center for redemption of monitoring offers, and crisis management and public relations costs.

Cyber Business Interruption

Covers financial loss when a company has its network-dependent revenue interrupted. Traditionally, this has been for fire, flood, etc., but technology growth has created new BI perils (viruses, tech failures, programming errors and computer hacking).

Hacker Damage

Covers costs to recreate or repair damaged or destroyed data, systems or programs.

Cyber Extortion

Covers the response costs and financial payments associated with the network-based ransom demands.

Multimedia Liability

Covers the costs to defend and resolve claims related to online content, such as defamation or trademark / copyright infringement.

The Bottom Line – The Coverage You Need

Many businesses operate for years without a serious insurance claim – much less a criminal event like a break-in or theft. But in the digital age, the likelihood of a being the target of a cyber crime is exponentially higher. Understanding your risks and getting the coverage you need can make all the difference. We're your Cyber Insurance experts – and we're ready to help you identify the coverage you need.