CYBER

Cyber Breaches Happen

With the increased use of e-commerce, web-based file storage, and the proliferation of smart phones, laptops, and tablets in businesses of all sizes, the risks associated with data security are growing quickly.

In 2015, over 169 million confidential records were exposed through more than 780 reported security breaches, according to the national nonprofit Identity Theft Resource Center (ITRC).

Cyber Liability coverage provides a comprehensive insurance solution to help your insureds from the moment a breech is suspected through restoration of their operations. Determining the appropriate limit of Cyber coverage for your client is easily accomplished through the five step process explained here.

Cyber Liability Insurance Highlights

- Legal Counsel Services
- IT security and forensic experts
- Public Relations / advertising support
- Breach notification
- Call Center and website support
- Credit monitoring and identity theft restoration services

Five Steps To Selling Cyber

1 Discuss data usage, storage and security.

Begin your introduction of cyber insurance by first gaining an understanding of your client's data management risks by asking questions like:

Where is the customer data stored?

Is the back up secured/encrypted?

By identifying these practices, you can help point out potentially weak links in your client's data management practices.

2 Identify number of customer records.

Many prospective insureds won't even know how many records they store! Why is the quantity of records so crucial?

Costs to respond to a data breach are directly proportional to the amount of records that are compromised. Based on industry research and expert advice, data breach response costs are approximately $10 to $30 per record.

3 Explain the costs of a breach.

Many insureds significantly underestimate how much a breach will cost, and think that they can self-insure it. Outlining what will happen in the event of a breach, with an estimate of cost, is very useful when explaining the value of Cyber.

Breach Costs 1: Legal Counsel
Breach Costs 2: IT Forensics
Breach Costs 3: Customer Notification
Breach Costs 4: Customer Call Center Support
Breach Costs 5: Credit Monitoring
Breach Costs 6: Public Relations Expenses

4 Review the causes of breach.

While the news headlines most often focus on data breaches affecting mega multinational corporations, the majority of reported breaches impact smaller businesses and result from accidental disclosures, lost laptops or improperly discarded files. The main purpose of this step is to make the insured understand that it can happen to them. There are four common causes of breaches you can quickly explain to your clients:

1. Negligence
2. Rogue Employees
3. Business Associates (third party billing agencies)
4. Hackers

5 Present insurance coverage.

Once you have discussed the potential risks to your client, introduce Cyber insurance. Discuss the coverage components that are most relevant to your client's business.

Help your client select a limit using the basic equation of: # of records x $20 (costs to respond)

Usually, when you compare the pricing for the Cyber to the potential cost of a breach, buying the coverage becomes a clear decision.

GENERAL AGENCY & Badger Mutual INSURANCE

CYBER

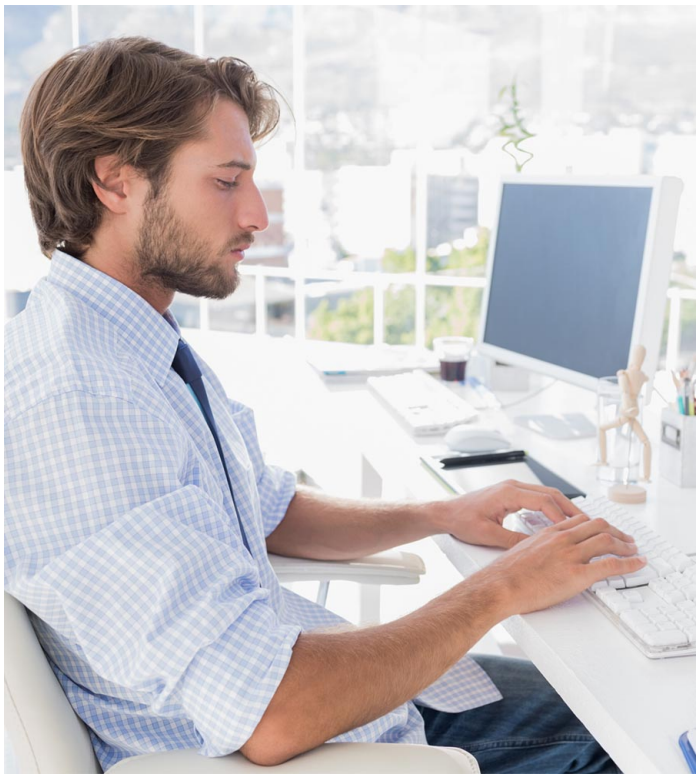
Claims Scenarios

Cyber Extortion

The manager at a popular local tavern, inadvertently downloaded an E-Mail attachment that appeared to be from his bookkeeper. The file contained the "CryptoLocker" virus that encrypted files on his computer, including the QuickBooks files that are used to manage the restaurants finances and payroll. When he tried to access an encrypted file, a message appeared that notified him that all files have been encrypted and will only be unlocked if he paid a "ransom" in BitCoin

After consulting with his insurance agent and their insurer, they were informed that this type of "cyber extortion" is covered by the cyber liability insurance policy. The restaurant manager engaged an IT expert referred by the insurance company and determined that the threat was real, and that the best course of action was to pay the ransom and assess further exposure and/or loss.

The ransom, IT costs and legal expenses amounting to almost $10,000 were covered by the restaurant's cyber liability insurance policy.



PCI DSS Assessment

Credit and debit card data from over 2,000 cardholders was exposed when a regional convenience store chain learned that 15 of its card readers (point of sale devices) had been compromised.

Across several store locations, the readers had been manipulated and credit card data had been skimmed by criminals and the information sold on the black market.

The investigation included the credit card companies, issuing banks, merchant banks and payment processors. Due to the issues at the stores, the credit card companies fined the stores for non-PCI-DSS compliance.