



Steps to Selling 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 2013, over **100 million** confidential records were exposed through more than 600 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 breach is suspected through **restoration** of their operations. Determining the appropriate limit of Cyber coverage for your client is easily accomplished through this simple five-step process.



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 key questions like:

How many customer records are there? Where is customer data stored? Is it encrypted? Do business partners have access?

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

Though many prospective insureds may not even know how many records they store, it is crucial to identify a ballpark number to be able to estimate the costs of a breach.

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 – \$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 the 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



Steps to Selling Cyber

4



REVIEW CAUSES OF BREACH

While the news headlines most often focus on data breaches affecting mega multinational corporations, the majority of reported breaches impact smaller business 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 4 common causes of breaches you can quickly explain to your clients:

- 1. Negligence (e.g., lost laptop or mobile device, improperly disposed files)**
- 2. Rogue Employees**
- 3. Business Associates (e.g 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 records x \$20 (costs to respond). Usually when you compare the pricing for Cyber to the potential cost of a breach, buying the coverage becomes a clear decision.