Cyber Security & Privacy Insurance

The Case for Cyber Insurance

Our increasing dependence on the Internet, email, and online databases may make us more efficient, but it also puts us at increased risk of sensitive materials falling into the wrong hands. Technology is changing daily and the ways in which information is collected, distributed, and even hacked, can change in an instant.

Cyber insurance (more accurately called information security and privacy liability insurance) is rated based on the amount of information at risk – number and size of records, nature of records, type of business or service provided, and revenue. Coverage differs from carrier to carrier, but these policies typically address both prevention ("pre-event") and reaction ("post-event") to data security breaches, and they often include valuable loss control and risk management services.

The value of digital data is often overlooked – until it is compromised. To better understand informational and digital assets, think of them as you would physical assets in any other risk management scenario. Having a full grasp and inventory of information collected, stored, or managed is the key to being prepared for any breach event.

5 Key Questions to Assess Cyber Exposure

Below are some of the key questions you should ask to understand the risks your Insureds face and to determine the type of coverage that's really needed.

1. What kinds of proprietary information do you collect, manage, or store?
2. What kinds of confidential personal information do you collect, manage, or store from your clients and your employees? Examples would include:
    a. Protected Card Information (credit card information, online commerce, etc.)
    b. Personal Healthcare Information (health records, social security numbers, etc.)
    c. Personal Information (name, address, age, driver's license numbers, income, insurance, etc.)
3. What kinds of confidential business information do you collect, manage, or store from your clients? (credit card information, banking information, address, revenues, other information subject to confidentiality agreements, etc.)
4. In what ways do you collect, store, or manage information? (i.e. paper files, electronic database or server, etc.) How is this information protected? (i.e. locked up, encrypted, etc.)
5. Do you employ third parties or outside vendors to handle proprietary information in any way? (i.e. document disposal, digital backup, etc.) Do you outsource any information technology?

Responding to a Cyber Crisis

Did a privacy breach occur? Was it a single event or ongoing? How many records were exposed? Now what? In which states do you have to notify individuals of the breach? What should those notifications say? Should you issue a press release?

CRC Insurance Services, Inc.™
www.crcins.com

Property | Casualty | Professional

PERFORMANCE IS THE DIFFERENCE™

Cyber Security & Privacy Insurance

Technology is complicated, and responding to a breach event is no different. The loss control and risk management services provided by carriers are invaluable in helping their insureds find the best experts (forensic, legal, public relations, etc.) to navigate these difficult issues. Reacting too quickly can cost more than necessary. So simply knowing who to call when a breach occurs can often help mitigate a crisis tremendously and provide peace of mind.

5 Key Questions to Assess Cyber Preparedness

To determine how prepared your Insureds are in the event of a cyber crisis, ask the following questions.

1. Who is responsible for information security with your organization? Does this individual oversee or select information-related third party vendors?
2. Do you have a formal information security policy in place? If so, are all employees trained on it?
3. What loss control initiatives are in place for information security?
4. Much like a formal disaster preparedness plan, do you have a formal procedure in place for a data breach incident?
    a. What is your formal process in notifying clients/customers of a potential breach?
    b. Are you aware of the state statutes regarding notification and regulatory compliance in a breach event?
    c. Are there funds set aside for these notification expenses, identity theft/credit monitoring services, and any public relations or advertising campaign to combat a bruised public image?
5. What is your protocol for lost electronics, such as cellphones or laptops? How would you address the loss of digital assets on such property?

Conclusion

Cyber insurance is still new territory and tends to be approached with hesitancy or even a bit of skepticism. The exposure is real, and it affects both large and small companies. Savvy companies are doing everything they can to protect their information assets, especially from a technology perspective. Our goal is to help you get the right information by asking the right questions when your Insureds ask about this thing called cyber liability.

To learn more about how we can help you, contact your CRC broker today.

CRC Insurance Services, Inc.™
www.crcins.com

Property | Casualty | Professional

PERFORMANCE IS THE DIFFERENCE™