What Every CISO Needs to Know About Cyber Insurance

One Page Summary

The impact of a cyber attack to an organization's brand, reputation, and business operations can be catastrophic. Organizations need to plan proactively but prepare for the reactive, which includes insurance for goods, intellectual property (IP), and commerce—the assets sailing across the digital landscape. Welcome cyber insurance.

EXECUTIVE SUMMARY

Symantec partnered with key thought leaders in the cyber insurance industry to compile essential information about cyber insurance in one report. Cyber attackers are more determined and persistent than ever before. Over half a billion personal records were stolen or lost in 2015 due to data breaches. Our industry experts' report, "What Every CISO Needs to Know About Cyber Insurance," provides information to help you lessen risk for your organization.

Legislative and Regulatory Update

Where there's smoke, there's fire. Major data breaches are in the news every day in both the private and public sectors; however, experts warn a massive cyber terrorist event could cause major market disruptions, and even physical damage to property and critical infrastructure. Congress and state and local governments are exploring ways cyber insurance legislation could reduce serious risks by encouraging safer cyber behavior.

Cyber Insurance: What You Should Know

Cyber insurance is evolving as fast as technology. What is considered core coverage today was not available as little as three years ago, and enhancements to coverage are negotiated in the marketplace every day. Cyber insurance itself is not a defense. It's the application of cyber insurance as another layer of defense, complementing the efforts of IT and other information security functions, where the greatest value is realized.

Privacy Attorney: Lynchpin to Success

When a data-privacy security incident happens, experts are needed immediately. The legal framework surrounding data security incidents changes constantly. It's not one-size-fits all. Proper legal handling of an incident requires counsel with significant data privacy experience. Those few attorneys who focus their practice in this rapidly growing area are the key to an organization's successful response to a crisis.

Insurance Brokers: More Than a Sales Contact

The insurance industry does not have all the answers today to identify and quantify cyber risks. To effectively assess cyber risk requires engaging an insurance broker. Unlike other classes of the industry, a broker represents the interests of you, the buyer. First-class brokers work with their clients to understand the assets at risk and how best to address them either under the existing insurance program or through a new dedicated product.

Incident Response: Why Planning for Failure Can Lead to Success

A major part of every cyber insurance claim is Incident Response. A well-built and regularly tested Incident Response program is an important component of a comprehensive risk management plan, and can mean the difference between a minor incident and a major breach. An Incident Response program should be in place long before you get into a compromising situation. Having live response provides better and faster results against attacks, allowing you to minimize potential data and monetary loss.

Crisis Communications in a Data Breach Event

A cyber attack can leave an organization helpless and its brand damaged. When compromised, companies have many different audiences they must reach in their communication. Often, organizations wrongly entrust crisis response to PR generalists, which is a dangerous gamble. Cybersecurity and breach response is fraught with legal and regulatory landmines that, if not understood, will likely result in lawsuits. Find a crisis communications professional to help you create a crisis communications plan.

Legal Viewpoint: How to Avoid Litigation

Companies should contact outside counsel as soon as they discover an information security breach. Under most state laws, the moment an organization discovers a breach is the time the clock starts ticking for the company to meet its legal obligations. Unfortunately, private litigation following the revelation of a breach seems inevitable. A company that can quickly discern the true impact of an attack will be in the best position to counter allegations.

LEARN MORE

For more information about how cyber insurance can protect you and your organization from risk, download the white paper: What Every CISO Needs to Know About Cyber Insurance.