NETWORKWORLD

IT BEST PRACTICES
By Linda Musthaler

About |
Linda Musthaler is a Principal Analyst with Essential Solutions Corp., which offers consulting services to computer industry and corporate clients to help define and fulfill the potential of IT.

Should you buy cyber insurance?

With the number breaches reaching an all-time high in 2014 many businesses are looking to mitigate risk with insurance

Network World | Dec 18, 2015 10:37 AM PT

This column is available in a weekly newsletter called IT Best Practices. Click here to subscribe.

Cyber insurance is rapidly becoming an important part of many organizations' risk mitigation strategy. While most businesses have some sort of property or general liability insurance, those policies exclude coverage for cyber liability, so cyber insurance has become its own category, and it's the fastest growing area of insurance for businesses. At least 50 major providers now offer this type of insurance, attracted by the fact that demand for cyber insurance has been rising by double digit percentages for the last few years.

According to the Insurance Information Institute, the number of reported data breaches reached an all-time high in 2014, exposing more than 85 million records. As those numbers grow, so does the interest in cyber insurance. Nearly half of all business owners carry some form of cyber insurance, but small businesses lag behind, largely because they don't see themselves as vulnerable to attack. However, breaches aren't always the result of a cyber attack; many data breaches stem from something as simple as the loss or theft of an unencrypted laptop or USB stick.

Industry pundits credit Target Corporation and Home Depot for raising the profile for cyber insurance. Since Target's disastrous data breach two years ago, the company has racked up breach-related expenses of $252 million so far. Of that, $90 million was recovered through insurance policies. Home Depot's expenses have tallied at least $232 million to date, and insurance has covered $100 million. CEOs and CFOs have taken notice of the benefits of having cyber insurance and are exploring the options.

BITS, the cyber security and policy arm of the Financial Services Roundtable, describes the value and importance of cyber insurance. Obviously it can offset many of the costs associated with an attack or breach, but insurance also is a risk-transfer mechanism. Cyber insurance allows a company to share the cost of an incident among a larger pool of insured companies. For the cost of a policy premium, company executives can have peace of mind that there is a safety net to sustain their business if something should happen.

The desire to have cyber insurance can be a motivating factor for a company to follow good cyber security practices and to have a strong defensive posture. Insurance providers don't want customers that are a big risk, so those seeking a policy (or at least one with good coverage and rates) must have their cyber security act together.

What cyber insurance typically covers, and what it doesn't

Insurance plans and coverage vary widely. According to the Financial Services Roundtable, there are four main types of cyber insurance coverage, including:

- Data breach and privacy management coverage, which covers the costs associated with managing and recovering from data breaches. This includes the forensic investigation, notification of victims of stolen data, credit monitoring for the victims, and associated legal fees.
- Multimedia liability coverage, which covers defacement of websites, media and intellectual property rights.
- Extortion liability coverage, which covers the damages incurred from extortion. For example, coverage might include the damages of having a hard disk encrypted by Cryptolocker or having a DDoS attack knock out a website or other services if a ransom isn't paid.
- Network security liability coverage, which covers incidents like third party theft and DDoS attacks.

Depending on how a policy is written, it might be expected to cover: revenue lost during a cyber attack; legal fees associated with a breach; the costs associated with fixing an exploited vulnerability; and credit monitoring for victims of a data breach.

What the insurance rarely covers is the loss of intellectual property such as product designs and business plans, since the insurance carrier can't accurately assess the cost of this type of loss. Also, losses that originate or occur within a company's supply chain might not be covered. A big area of exclusions stems from intrusions and data breaches that are the result of cyber warfare directed by state actors and terrorists. Most cyber as well as general liability policies exclude coverage for losses arising from war and terrorism.

A company that is buying insurance should have an attorney look at what is what is covered and what isn't. For example, a policy could be written such that the organization may not be covered for employee-owned devices that could be the cause of the breach. This would have huge implications for

a company's BYOD policies and protections.

How to get the most from your policy

Al Berman, president of Disaster Recovery Institute (DRI) Inc., says companies must really do their homework to understand what they need.

The first step is to do a risk assessment and impact analysis. Companies must understand where their risks are and what the impact of a breach would be on their business. For example, if a regulated company has a data breach, it might be required by law to notify individuals that their data was stolen, and the notification process can be quite expensive. However, if the company is not regulated and not mandated by law to report the data loss, the impact of the breach could be minimal. A thorough impact analysis will help to understand what kind of coverage, and how much, is necessary.

When an incident occurs and a claim is made, the policy holder must understand the requirements for proof of the event. For example, a forensic investigation may be required to determine if the breach was tied to a state-sponsored cyber attack, which could be excluded from coverage.

Berman stresses the need for legal counsel when selecting a policy. A lot can be at stake and the wording of a policy can be the difference between a large payout and deniability of a claim.

Cyber insurance is not a substitute for making smart investments in cyber security and following industry best practices. However, it is an important part of almost any business' risk mitigation strategy.

Linda Musthaler

Linda Musthaler is a Principal Analyst with Essential Solutions Corp. which researches the practical value of information technology and how it can make individual workers and entire organizations more productive. Essential Solutions offers consulting services to computer industry and corporate clients to help define and fulfill the potential of IT.

Must read: 11 hidden tips and tweaks for Windows 10

View Comments

YOU MIGHT LIKE