Are You Really Covered by Your Cyber Insurance?

February 15, 2019  |  By Mike Elgan

The whole point of IT security is to minimize risk, and risk is, ultimately, a financial reality. A well-run organization practices risk mitigation by not only using the best tools, services and methods for maximizing data security, but also increasingly by augmenting great security with the right cyber insurance.

As we know, the cyberthreat landscape is in a constant state of change. It’s a contest between evolving threats on the one side, and the security knowledge, options, resources, products and services on the other. The insurance landscape is also in a constant state of change. Yet too many organizations treat this kind of insurance as either unnecessary, or as a necessary, but generic, turn-key, set-it-and-forget-it checkbox item. In fact, it’s an important, complicated and necessary financial service that needs to be frequently reviewed, reconsidered and updated.

With new and evolving threats to your organization’s financial well-being, it’s time to rethink what you know about cyber insurance.

Why Most Companies Aren’t Covered

Cyber insurance is a relatively new phenomenon for most companies. Only 38 percent of organizations are covered by data insurance, according to Spiceworks, a social exchange for IT services. Of those covered, around 45 percent have had coverage for less than two years and only 24 percent have been covered for more than five years. Furthermore, only 11 percent of those without insurance plan to buy a policy within the next two years.

That means knowledge about and experience with insurance is understandably incomplete at most organizations. As a result, corporate leadership is often unsure about its value or about the specifics of coverage.

Unfamiliarity with the finer points of insurance is also evident in the Spiceworks survey. Of the organizations not covered, the top reasons for not yet purchasing cyber insurance are that it just isn’t a priority at the organization (41 percent), a lack of budget (40 percent), a lack of knowledge about insurance (36 percent), and it’s simply not required by regulations at the organization (34 percent).

This lack of understanding is very troublesome given the average total cost of a data breach ranges from $2.2 million to $6.9 million, according to the “2018 Cost of a Data Breach Study” from the Ponemon Insitute and IBM Security. For bigger breaches at larger companies, the cost can soar into the hundreds of millions of dollars.

A wide gap exists between the actual need for insurance and the perceived need. It’s time to change that.

https://securityintelligence.com/are-you-really-covered-by-your-cyber-insurance/
Insurance Against Hacks? You Don’t Know the Half of It

Most people in the industry would say that the point of cyber insurance is to protect against the financial hit from an attack, right? This may be true, but not always.

Verizon’s “2018 Data Breach Investigations Report” investigated more than 53,000 incidents and more than 2,000 confirmed breaches. They found that around 73 percent of data breaches took place because of external attackers, while 28 percent involved employees and other insiders.

Unfortunately, insurance coverage sometimes focuses on external hacks to the exclusion of “inside jobs,” accidents, service provider errors and other non-hacking causes.

Going back to the Spiceworks report, policies can vary greatly: Liability is covered by 78 percent of cyber insurance policies, electronic data by 75 percent and legal or investigative fees by 69 percent. But only around 52 percent of those policies cover loss of income or cyber extortion losses, and only 35 percent cover damage to reputation.

In addition, according to U.K. insurance governance company Mactavish, many insurance policies contain eight major flaws:

1. They cover attacks or hacks, but may not cover accidents and errors;  
2. They cover only costs required by law, but may not cover the total incident costs;  
3. Coverage is limited to the time of the network interruption, but may not cover business disruption;  
4. They may limit or exclude systems delivered by outsourced service providers;  
5. They may exclude software or systems in development or beta;  
6. They may not cover incidents caused by contractors;  
7. Notification requirements may be too complicated; and  
8. They may only cover insurer-appointed advisers and specialists.

When considering your options for cyber insurance, keep an eye out for these common exceptions to ensure you’re picking the plan that best fits your business needs.

How Compliance Complicates Coverage

In addition to focusing on data breaches, organizations must pay attention to a complex and evolving regulatory environment. Enterprises now face a new world of regulatory compliance around privacy, from the General Data Protection Regulation (GDPR) to the California Consumer Protection Act (CCPA), which will go into effect on Jan. 1, 2020.

It’s tempting to respond to this by saying, “We’ll just comply, of course, and all will be well.” But it’s not that simple. Fines for noncompliance could be enormous, and companies can be fined for not only violations or potential violations of user privacy, but also for how personal data is collected, stored, processed and even how the collection is communicated to the public.

https://securityintelligence.com/are-you-really-covered-by-your-cyber-insurance/
All this is new, and it’s likely that in the coming years, many organizations will be slapped with hefty fines for misunderstanding the laws’ fine print, how they express and organize their privacy policies, how user data is processed, and other peripheral or secondary matters.

Bringing it back to cyber insurance, many policies will not cover fines or other costs if the violation is around the processing of data or communication of policy. Some U.S. states even ban insurance coverage for regulatory fines of any kind, and insurance companies strike that coverage in those states. Compliance is becoming an increasingly relevant aspect of insurance, but many insurance policies just don’t fully cover it.

**It’s Often a Matter of Interpretation**

One problem with an unsophisticated approach to insurance is that organizations can accept policies that don’t cover them. Another problem is having a different interpretation of those policies than the provider, which can be a costly misunderstanding.

One interesting example is what I call the “act of war” clause: Many policies will cover a breach, unless that breach is the result of an “act of war” by a nation state.

That sounds reasonable. The trouble is, some of the most sophisticated and damaging exploits are developed by these threat actors. Some are created by one government, modified by another, then deployed by who-knows. This could provide a loophole for insurance providers that don’t want to pay up. They can argue that a hack enabled by malware developed by a foreign government means the attack was an “act of war,” and therefore not covered under the policy.

**How to Find Cyber Insurance Coverage That Fits**

The important takeaway here is to not make assumptions about coverage. Read the fine print. Pay special attention to liabilities around compliance, including fines.

Ideally, the right insurance offers cyber risk mitigation that offsets some or all of the costs when recovering from a breach or other security event. The right policy will compensate for not only lost business during business or network interruption, but also lawsuits and even extortion costs.

It’s also important to understand that insurance won’t cover you if you’re not protecting yourself with great security software, systems and policies. If your company is negligent with security, the insurance companies won’t pay.

First, make sure you’ve got strong cybersecurity systems, tools and procedures in place. Then, shop around for the cyber insurance plan that works best for you — and read the fine print. Negotiate for a policy that truly and fully covers all possible financial loss for everything having to do with data — from attacks to accidents to compliance. Lastly, review your coverage regularly as cyber risks evolve.