

A Cyber Liability Endorsement Vs. A Cyber Liability Insurance Policy – What You Need to Know ...

What should business owners be **WARY OF** when opting for a cyber endorsement instead of a stand-alone policy?



Coverage Limits Are Too Low

Cyber endorsements typically have a much lower limit of liability available than a stand-alone policy. Depending upon things like your class of business, your annual revenue, the number of records you store, and how your business operates (statewide, nationally, internationally) an endorsement may not be right for your needs.



Where's the Third-Party Coverage?

Most common on a cyber liability endorsement added to a commercial package policy, the insured will often lack coverage for third-party losses. Only first-party losses will have coverage, but even this coverage can be limited.

What does that mean? First-party coverage pertains to loss or damage sustained by an insured to its property. What about loss or damage sustained by a third-party that your cyber-related event causes? If a third-party claim is made and you don't have coverage, you could be left footing a bill that your business is not prepared to pay. In short, different interests are protected by first-party coverage and third-party coverage. An endorsement may not be enough for your needs.



On the Contrary, Where's the First-Party Coverage?

More commonly on endorsements to a professional liability policy, only third-party coverage may be included and if first-party is included, it almost always comes with much lower limits. Without adequate or any coverage for first-party losses, you could be looking at a self-pay bill that will quickly add up for things like forensic investigation to determine the source of the breach and stop it. Also, you will most likely require the repair of damaged or lost electronic data and you'll have to contend with state compliance requirements of breach notice reporting, which comes with a hefty cost. These are just a few of the significant costs involved in a cyber-related event.



Event Response Services, aka Breach Coaching, Can Be Inadequate or Not Included

The increasing complexity of data breaches is a sign of the times. Therefore, the role of an event response coach, otherwise referred to as a breach coach, is a critical part of managing a cyber-related event. They help companies understand the tasks that need to take place, the timeliness of when they need to take place, and they know and understand the regulatory climate for each different state regarding notification requirements and more. This in itself could be a crippling task and expense if a company operates nationwide and you don't have event response services. Unfortunately, cyber endorsements often limit or don't provide coverage at all for this service. A stand-alone cyber policy has much broader coverage.



The Cost of a Cyber Liability Policy

Often, business owners assume that this coverage can be too expensive to purchase. However, when it comes to small and mid-sized businesses, depending upon things like your class of business, your annual revenue, the number of records you store, and your past claims history, cyber policies are affordable and range around \$800 annually up to around \$7500.



The Cost of a Claim – An Average Case Scenario

The cost versus the risk is an important consideration. If you consider how much a cyber-related event could cost you financially alone, the investment in your protection is well worth it. For example, in a case where **2000 client credit card records** were exposed the following costs were incurred: Investigative costs: \$30,600 ► Managing the crisis and reaching out to customers and the public: \$23,850 ► Payment Card Industry – Data Security Standard (PCI-DSS): \$29,000 ► State and federal authorities: \$2,660 ► **Total cost: \$194,390 | Total cost per record: \$97.** Let's add in the inevitable, "the attorneys are coming with a class action lawsuit" **Lawsuit cost: \$582,160 | Total cost: \$784,950 | Total cost per record now: \$392**