Four Reasons a Cyber Claim Could be DENIED

Navigating the waters of Cyber liability claims can be complex and confusing for policyholders.

Events that may trigger a claim are sometimes nebulous, such as when a data breach is suspected but not yet confirmed. Insureds, especially those with little or no technology savvy, might also have difficulty getting claims approved if they have been slow to identify and address potential threats.

A business also could see its claim denied if it is not familiar with policy exclusions and requirements.

Getting the most out of your Cyber coverage means making sure a claim gets covered when a breach or security event occurs. By understanding the most common reasons Cyber claims are likely to be denied, you will be better prepared to get claims successfully resolved.

1. Late or improper notification

Late notice is perhaps the single most common reason a Cyber claim is denied by a carrier.

This is particularly true if a policy is written as claims-made-and-reported, as many Cyber liability policies are written. Unless the policy has specific language that allows claims for a period of time after the policy ends (usually limited to just a few months at most), then notification during the policy period is key to getting these claims approved. In addition, notice of any occurrence that could lead to a claim also must be made to the carrier in a timely and appropriate manner. Lagging on the alert to an insurer in any instance where claims activity could follow is setting the policyholder up for a denial.

Because Insureds who fail to submit their Cyber claims on time are among the most likely to find their claims denied, they should be made acutely aware of the need for timely notification of any potential claims activity. This enables them to establish important workable protocols internally.

Delays by IT or other internal groups in alerting the risk management contact, for example, could jeopardize an eventual claim. And because cyber threats can enter an organization through a number of avenues, the organization's processes must be established in a way that minimizes potential delays.

2. Lack of understanding on coverages

Cyber liability policies don't all cover the same types of losses.

It's crucial that policyholders understand which coverages they require and which they actually have. Agents and brokers should work with each client to ensure they've been matched with a policy that covers those types of exposures they're most likely to encounter. This may be dependent on a variety of risk factors, including industry, type of business (online versus brick-and-mortar, etc.) and type of technology or data assets that must be protected.

Policyholders also should be aware of their responsibilities under the coverage they've selected. This may include applying security patches, using encryption technology or other measures.

If the organization isn't in compliance with these mandates, their claim could be denied by the insurer.

Other types of coverages also vary from one Cyber policy to another. Legal support may be included in some, but excluded in others. The purchase of any technology tools necessary to remediate an exposure aren't always covered. A small business with sparse internal IT expertise is likely to have very different expectations than a large, tech-savvy consulting firm. If a policy isn't closely tailored to the client's needs, they may find their claims denied.

3. **Exclusions within contract language with third party vendors and clients/customers**

Many businesses rely on third parties to provide a variety of services, such as payroll processing, cloud hosting and teleconferencing. Similarly, those that generate revenue in the business-to-business space have other companies as their clients. Whether their role is as a customer or a vendor, these relationships have the potential to send the policyholder into a situation where their coverage may not follow.

A claim related to an exposure that occurred while sharing data with vendors, for example, may not be covered. System connections to a client's network might fall outside the scope of the policyholder's plan. Even the method of exposure could prompt a claim to be denied. Fraudulent entry into one area of the network may be covered, while a compromise in other areas or through specific systems are excluded.

To avoid an unexpected claims denial, it's vital that policyholders review all contracts they enter into with vendors and clients alike.

This step will ensure their cyber policy will provide coverage to the extent they are agreeing to in their contracts. Is the information stored outside the organization's network included in the policy? Will externally generated data be covered if a breach occurs within the policyholder's system? It's common to assume that a claim for either of these scenarios would be approved, but that may not be the case. Understanding limitations and exclusions of the policy is key to a successful claim.

4. **Not involving the carrier early enough, i.e. risk management (identifying potential risks) or suspicion of exposure**

Producers and policyholders have a great resource available to them in the form of the carrier, and when in doubt, claims — even those involving questions or uncertainty — should be reported as quickly as possible. This allows the carrier to investigate and determine if there is any exposure.

Policyholders will then have the concrete information they need to know they are not taking on undue risks. When Insureds wait to notify the insurer, there are more likely to be potential showstoppers that result in the denial of a claim.

Call the experts at R.G. McGraw Insurance for an analysis of your business Cyber Risks and Coverages to obtain the insurance you need. 513-381-7881

Source:
4 Reasons your Insureds Cyber Claim could be Denied
Feb 02, 2016 |By Joe Salpietro