Warning: Cyber Liability – Increased Risk With COVID-19

Insights by Zach Slade

How does the Coronavirus Change Cyber Liability Exposure?

Experts are projecting a **30-40 percent increase in cyber attacks** during the novel coronavirus pandemic. This is primarily due to hackers exploiting the vulnerabilities associated with this crisis, especially those arising from employees working from home. In situations such as these, companies need to reexamine their network security infrastructure and Cyber Liability Insurance program. The following questions should be asked:

1. **Do we have Cyber Liability Insurance?** – Data from 2019 suggests about 50 percent of middle market companies do not have this coverage.

2. **If so, do we have the appropriate Cyber Liability coverage?** – More on this below. However, know that Cyber coverage is non-standardized and varies from carrier to carrier (and sometimes even within).

Contract language is important! The average cost of a data breach has exceeded $1 million and, unsurprisingly, many purchasing Cyber Insurance still don't understand what is covered. It's not uncommon for Cyber Insurance policies to contain exclusions that could result in claim denial.

For example, a review the Cyber policy for a law firm now encouraging all employees to work remotely, revealed that the firm's Cyber Insurance Policy specifically excluded any attack originating from an "Unencrypted Mobile Device," which is likely the very place hackers are now targeting! We never like seeing this exclusion, but it's especially important to be aware of any limitations during this time of change and uncertainty.

The good news is, a well-written Cyber Insurance Policy will pick up the additional liabilities associated with this exposure. However, since contract language is so inconsistent, we recommend reviewing your policy carefully and paying attention to any limitations. A few key areas to focus on include, but in no way are limited to, the following:

- **'Unencrypted Mobile Device' Exclusions** – Should not be present in the policy as referenced in the example above.
- **Social Engineering/Cyber-Crime Coverage** – Anticipate a surge in these claims due to COVID-19 (scams, phishing, etc.)! Make sure this coverage section is included, terms are broad, you're aware of any sub-limits, and these crazy "Call Back" or "Out of Band" conditions that could prevent coverage are not present in the policy.
- **Employee Owned Device Coverage** – Make sure coverage clearly extends to these devices.
- **Ransomware** – Confirm coverage and know how your policy would respond.

If your company is purchasing Cyber Insurance included via endorsement in a General Liability package, you should be extra careful. It's important to know that **every company has some existing cyber exposure that needs to be understood**. Furthermore, it's often the industries that have historically not prioritized Cyber coverage because of their lower exposure that are now being targeted. All companies should be reevaluating their posture when it comes to Cyber Liability and understand the increased risk associated with business changes such as employees working remotely.

We recommend working closely with a trusted IT professional while making this transition. That said, given the new vulnerability of endpoints and human error, it's projected this change in behavior will result in a large increase of successful cyber attacks. **Every company should understand its own insurance response to a data breach** should they be affected by this increased effort from cyber criminals.

ALERAGROUP