Remote Workforce and Cyber Insurance:

Are They In-Sync?

By: Lee Lazar

With millions of people working remotely in observance of "stay at home" orders across the country, business owners and information technology managers have a new set of risks to manage regarding how their data is secured, controlled, and accessed. One set of issues that must be considered is how a company's cyber insurance policy will respond in the event of a data breach against an employee's computer, cell phone, or other device. Insurance companies design policies to provide coverage for employees working from home; however, these policies include many restrictions that can prevent a claim from being paid.

Our team of advisors is educating clients on their policies and best risk management practices. The goal of these conversations is to create a secure environment for remote computing that will be in compliance with their policy.

The four topics below are some of the most common examples of where cyber policies may be in conflict with your employees' work from home routine:

1) **"Owned and Operated" language** – Many cyber policies contain "owned and operated" language, meaning coverage is NOT provided if an employee's personal device containing company files is hacked.
2) **The network matters** – Coverage may not be available if a breach occurs across an employee's home internet or unsecured Wi-Fi signal. Make sure you understand the nuances of your company's policy and implement procedures accordingly.
3) **Non-business activities can compromise coverage** – Many policies will not cover a data breach caused by personal websites or the use of a business device by a child at home. Under these terms, devices used for business should not be used for any other purpose.
4) **Create a "bring your own device" policy (BYOD)** – Some cyber policies will extend coverage to all devices, but only if your business has a BYOD policy in place that is signed by all employees. HR Managers should be engaged to make sure proper procedures are in place and signed off on.

The list above is only a sample of the many restrictions that may appear in cyber policies. Please reach out to a member of our team so that we may assess your cyber policies and current situation. We will help your business build a plan that balances your insurance policy provisions with digital risk management during this unprecedented time.

About The Author: Lee Lazar has been an Insurance and Risk Management Advisor with Associated for over 11 years. Cyber insurance & digital risk management are a primary area of focus for his practice.