6 Common Misconceptions about Purchasing Cyber Insurance

You may be thinking, why do I need cyber liability insurance? Or, is it worth the additional cost in premium? These common misconceptions will shed light on the importance of purchasing a cyber insurance policy and the potential risks of not having one in place.

1. I'm not responsible because I outsource.
According to state and federal privacy laws, the obligation to protect personal records remains with you and your customer. Your customers have no relationship with the third-party vendors you use. Even though a third-party vendor may be responsible for losing confidential information, they are working on your behalf and therefore, you are responsible for responding to your customer. You may be able to get financial assistance from a third party for a loss they've caused, but they could potentially harm your customer relationship in their response to the cyber event.

2. I use paper records, so a cyber liability policy won't help me.
Privacy laws apply to protected health Information (PHI), personally identifiable information (PII) and other protected information stored in any format, including paper. Cyber liability insurance also applies to protected information stored in any format, including paper.

3. I'm covered on someone else's policy.
Danger lurks behind this assumption. The other party's policy may not cover you for your own expenses and liabilities. An additional insured endorsement on someone else's policy may only cover that other party's liability to you. Not all cyber liability policies will address exposures applicable to your organization.

4. I have a contract that will provide protection.
Indemnification from a contract is often limited to circumstances involving or caused by the other party in the contract. It is unlikely that the other party will indemnify you for your own mistakes or breaches. You would also need certainty that the other party has the means to assist you and no "out" clauses. Relying on a contract adds the additional burden of suing another party for breach of contract in the event they offer limited to no assistance.

5. My business is too small to be a target.
Hackers know that smaller organizations may not have adequate IT infrastructure, which makes them a more desirable target. They also know that smaller organizations cannot afford to be offline very long, which might make them more inclined to pay ransom demands to recover systems and data. In fact, 43% of all cyber-attacks target small business.

6. I have coverage on my other insurance policies.
Due to past ambiguity in policy language, some cyber claims were covered by non-cyber insurance policies. Most non-cyber policies now have exclusions to make it clearer that cyber losses are not covered anywhere but a dedicated cyber liability policy. Even if there is some unintentional coverage on a non-cyber policy, the other policy terms and conditions will greatly limit the coverage available to you.

Other policies are designed to cover bodily injury, property damage, third-party damages, theft of funds by employees and advertising injury arising from anything you publish. Those policies are not designed to respond to losses from ransomware, social engineering, data spills, network interruptions, bricked electronic devices, responding to regulators, notifying potential victims, paying for credit monitoring, fraud resolution services, and many other coverage features included in a cyber liability policy.