What Does a Cyber Insurance Policy Cover?

While cyber insurance has always been vitally important to businesses, it is now more important than ever. With more employees working remotely and utilizing technology to virtually assist customers, businesses are facing more cyber exposure. The good news is cyber insurance policies are available to address these exposures. So what kind of things does a cyber policy cover? I will go over some of the coverages included in a "standard" cyber policy. This is not an exhaustive list of coverages, conditions and exclusions. Before purchasing a cyber policy, I recommend going over specific terms and conditions with an insurance professional.

When it comes to cyber insurance coverage, cyber incident response coverage is an extremely important part of the cyber policy. This coverage helps a business gain advice and consultancy, obtain remote support and assistance and coordinate an initial response to a cyber event. I highly recommend purchasing a cyber policy from a company that has their own cyber response/claim department. This helps streamline the process of a cyber event and saves a business owner the burden of finding their own cyber event specialists.

Privacy liability and network security liability are what most people see in the news when it comes to cyber incidents. We have all seen news stories where a large retailer has had a cyber event where customers' personal information has potentially been compromised. These kind of events are covered under the privacy liability and network security liability sections of the cyber policy. The cyber policy can provide coverage when a cyber incident has potentially led to unauthorized disclosure or access to personally identifiable information or protected health information of others. This can include direct financial damages suffered by an affected party as well as expenses such as legally required notifications to possibly affected individuals, credit monitoring for possibly affected individuals and a temporary call center to manage calls related to the cyber event. Network security liability coverage can also provide coverage if your network is used to transmit malware to a third party's computer system or used to carry out a denial of service attack.

The cyber policy can also provide coverage for regulatory fines and PCI fines, penalties and assessments. For any business taking credit cards, the PCI piece of coverage is especially significant. Many business owners mistakenly think there is broad coverage for cyber events through their PCI vendor. All business owners need to read their credit card processing agreements very closely. When you do, you will notice lots of hold harmless language in favor of the PCI vendor. A cyber policy can help fill in these gaps.

Cyber crime coverage is a part of the cyber policy that has seen an increased frequency of claims. The funds transfer fraud section of the policy provides coverage for unauthorized electronic funds transfers from your bank, theft of money from your bank by electronic means and theft from your corporate cards by electronic means.

Phishing and social engineering have also become much more prevalent. Examples of these type of incidents would be an employee paying a vendor invoice that was e-mailed to them that ended being fraudulent or an employee sending money per instructions of an e-mail from a business owner where

the e-mail was actually fraudulent. Cyber criminals have become very sophisticated in making fake e-mails and requests appear legitimate.

Extortion coverage on the cyber policy is also commonly known as ransomware. In these cyber events, a business owner will receive a threat requiring a payment within a certain period of time. If the ransom demand is not met the cyber extortionist may unleash a virus that will crash the business' computer system, cause damage to specific programs or revel confidential information entrusted to the business.

There are many more coverages included on a cyber policy, but I would consider these the "universal" coverages that will apply to most if not all businesses. If you would like a consultation to analyze your cyber risks and how a cyber policy can provide protection from those threats, please contact me.

Dan Gabel, CRIS
Partner, Shore Murphy & Associates of Casey
Office: (217) 932-2267
Cell: (217) 962-0461
E-mail: dan@shoremurphycasey.com