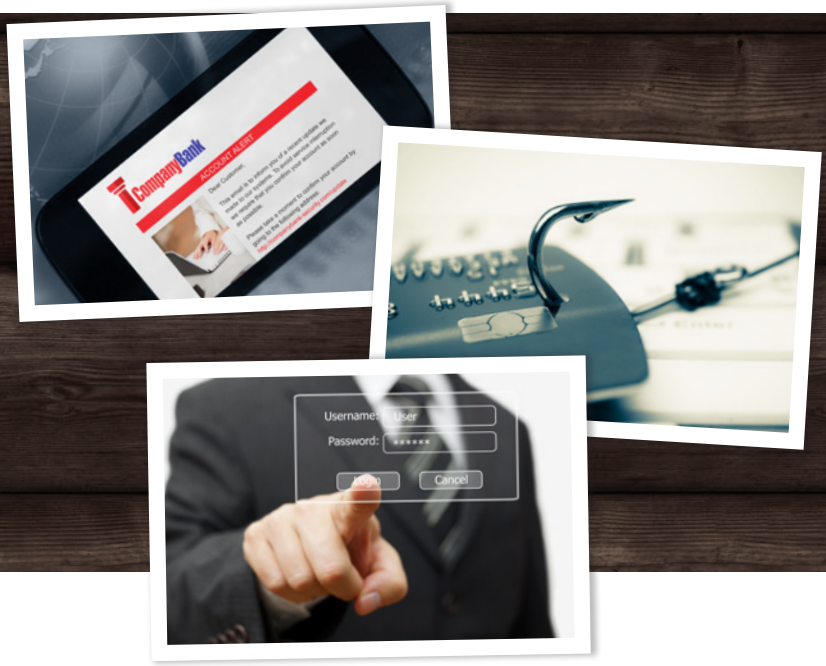
PARKER | SMITH | FEEK

COMMERCIAL INSURANCE
EMPLOYEE BENEFITS
PERSONAL INSURANCE
RISK MANAGEMENT
SURETY



CYBER SECURITY

SEPTEMBER 6, 2017

CYBER INSURANCE PROTECTS COMPANY AND CLIENT INFORMATION FROM ATTACKS

Gregor Hodgson | Vice President, Account Executive

Every week we hear of a new virus, hack, or ransomware that threatens our business operations or employee or client information. Many business owners have been hearing about, and are now considering, cyber insurance. But, what exactly is cyber insurance? What does it cover, and is it a good fit for my business?

In order to understand what cyber insurance covers, we first must understand what constitutes a cyber incident. A good definition of a cyber incident is, "The failure to prevent the theft, loss, or disclosure of personally identifiable, non-public information (or corporate information, which you have a written obligation to protect) that is in the care, custody, or control of your organization or a third party, for whom you are legally liable." This definition covers:

- Loss of a laptop.
- Hack of a POS system.
- Phishing schemes that trick an employee into divulging personal information to others.
- A hacker who steals data and then extorts your organization by threatening to release the data, or by encrypting the data and offering to sell you a key.

Whatever the circumstances, cyber insurance can help you assess the damage, respond to the initial threats, and manage the fallout of such an event.

When a hack is discovered, an organization must first identify what has happened and assess the possible damages. According to the Ponemon Institute's "2017 Cost of a Data Breach Study," which analyzed more 419 breaches, the mean time that it took an organization to identify a breach was more than 190 days and the mean time to contain a breach was more than 65 days.

> ...cyber insurance can help you assess the damage, respond to the initial threats, and manage the fallout of such an event.

Given this lag time, an IT forensic firm is often needed to discover what happened, what information was accessed, how the organizations' servers were co-opted, and what patches are required to correct the problems. Once the forensic firm can identify what information was accessed, then legal counsel is engaged to identify regulatory and other reporting requirements.

continued >

Forty-eight states now have breach notifications laws, not to mention federal legislation as well as foreign breach notifications statutes that may trigger an organization's need to respond. Notification requirements could include various state attorneys general, federal agencies, bankcard issuers, business partners, and the many individuals whose information was accessed. Legal counsel is needed to sort through the myriad of reporting requirements and to prepare a response. By hiring legal counsel to conduct the investigations, an organization will be better positioned to keep the findings of the investigation subject to attorney client privilege and confidential.

Once damages have been assessed, the initial response to the breach can begin. As mentioned above, depending on the size and scope of the breach, state and federal agencies may need to be notified.

If credit card information was accessed, organizations may be required to demonstrate PCI compliance. If social security numbers, health information, or other personal information is compromised, organizations need to begin informing individuals affected by the breach.

Depending on the jurisdiction and extent of the breach, credit-monitoring services may need to be provided to those impacted. If the breach included data corruption and extortion demands, then the organization must decide whether they are going to negotiate with the extortionists or if they can recreate needed data from back-up systems.

And finally, if news of the breach has reached the public, then public relation or crisis management services may be needed in order to communicate with customers and the general public.

Once the initial response is contained, the organization can turn to managing the fallout of the attack. This may include class action lawsuits, regulatory or PCI fines, data restoration, income loss, as well as rebuilding a damaged brand.

A well-structured cyber insurance policy can help an organization address all of the challenges outlined above. In addition to the financial protection, most insurance carriers now offer data breach coaches, who help the organization manage the entire project. These coaches, often lawyers with extensive cyber experience, provide significant value to an organization that has fallen victim to a breach.

> [Cyber insurance] policies are far from standard contracts and most need to be customized to fit the unique exposures faced by your organization.

Having managed hundreds, if not thousands, of breaches, the data breach coaches can help the victim organization navigate the many perils and pitfalls faced while responding to a breach. Their experience can be invaluable as you attempt to negotiate the regulatory and business challenges of a breach.

In addition to the financial protection and consultative assistance, most insurance carriers are now offering pre-breach services that an organization can use to prevent, as well as to prepare for, an inevitable incident. These services include sample data breach response plans, insurance limit analysis, discounted virus detection software and employee training, table top exercises, and more.

The market for cyber insurance is rapidly expanding. However, the policies are far from standard contracts and most need to be customized to fit the unique exposures faced by your organization. Consult with your insurance broker and discover the value of a comprehensive cyber insurance program.