MITIGATING CYBERSECURITY RISK VIA INSURANCE

Cyber insurance is now a 'must-have.' Make sure you and your insurance professional understand its many moving parts.

By Paul J. Smith

KENTOH / SHUTTERSTOCK.COM

RAWPIXEL.COM / SHUTTERSTOCK.COM

Sooner or later, any business that handles customer data will be confronted with the challenge of a data breach. As we have all heard: It's not a matter of "if" but "when."

The pain points following a breach of client data are numerous, and responding properly to the many "moving parts" of a breach is difficult for the most expert teams, especially small ones. How many small firms have the forensics expertise to research firewalls, networks, endpoints, mobile devices, etc. — under the pressure of a burning fire — assuming for the moment that they have the capital resources to move quickly to mitigate the damage?

Of course, the larger the firm, the more likely it is that internal or outsourced experts are available. But even at the largest companies, fumbling the first steps of a breach response is common, if not inevitable. After all, depending on the moving parts, it's likely the firm's IT team has never encountered a major breach or event. And if all clients' personally identifying information (PII) has been breached, the response must be quick and conducted in accordance with state law in each state where a client is located.

BREACH RESPONSE COVERAGE

It may come as a surprise to some readers that for most small to mid-size firms, the appropriate first call may be to the insurance carrier, assuming there is coverage with one of the major carriers that have a breach response team available 24 hours a day.

The better cyber insurance policies will include support where the insured can receive immediate expert help with IT expertise, privacy attorneys and technical experts. For larger firms, coverage can be designed to support the in-house team at designated levels, depending on the breach specifics.

This kind of breach response assistance is an important resource provided by most cyber insurance policies. It is what's referred to as first-party coverage — you are not being sued (yet), but you do need forensics, call center help and access to other resources immediately. These resources include:

- Loss of digital assets coverage
- Business interruption and extra expense coverage
- Cyber extortion/ransomware
- Public relations

Let's take a closer look at those four key resources.

Loss of Digital Assets Coverage

This provides coverage for the costs to replace or restore electronic data that was damaged in a hack, via virus, malicious instructions or a denial-of-service attack (i.e., ransomware) that was inflicted on the policyholder with the intent to damage, delete or corrupt its ability to operate normally.

Business Interruption Coverage

This provides coverage by way of reimbursement for the actual loss of the policyholder's business income or additional expenses in connection with a covered loss (i.e., a virus, malicious instructions or a denial-of-service attack inflicted on the insured's computer system that was designed to damage, delete, destroy, corrupt or prevent access to any part of the system).

Cyber Extortion/ Ransomware Coverage

This provides reimbursement of pre-approved extortion expenses and ransom payments that result from a cyber extortion event, including threats to destroy or prevent the normal use or access to the insured's computer system. This is an example of when it is critically important that the policyholder and the carrier begin communicating immediately.

Public Relations Expense

This provides for the reimbursement of reasonable expenses of an insured to restore its reputation resulting from negative news coverage and publicity in connection with a covered event. This loss scenario should not be underestimated — recovering from reputational damage following a breach can be challenging.

Today, breach response coverage is no longer a luxury — it's an essential and required part of a readiness program. Offloading a significant part of a firm's breach response liability to a cyber insurance carrier is becoming standard practice.

THIRD-PARTY COVERAGE

The first-party coverages described above would be available to the insured without a third-party claim made against them. Many readers are more familiar with "claims made" coverage that's designed to respond to client claims against the insured with defense expenses and payment of covered damages. For example, professional liability insurance is a familiar coverage that in most cases would only respond to a written claim for damages inflicted on a third party — that is, a client of the insured.

Third-party claims are less predictable, given the nature of their origin. They occur when a harmed party sues an insured for harm done

by a wrongful act (generally as defined in the policy) as a result of neglect, breach of duty or omission in maintaining the security of the insured's computer system, such that a non-insured person:

- gains access and causes harm to the insured's clients;
- publishes the PII of the insured's clients; and/or
- uses an insured's computer to transmit a virus to a third party who then files suit against the insured.

Typical third-party claims that would be covered by a cyber insurance policy include website liability, media liability, regulatory proceedings, class action lawsuits, and payment card industry (PCI) fines.

Website Publishing Liability Coverage

This would be triggered by a third-party claim of a wrongful or harmful statement published on the insured's website where the published material included alleged errors, misstatements and/or copyright and privacy violations; and for defamation, libel, slander, trade libel, infliction of emotional distress, outrage, outrageous conduct or other tort related to disparagement or harm to the reputation or character of any person or organization.

Media Liability Coverage

This would cover an error or omission arising out of publishing or broadcasting the insured's content, where a wrongful act third-party claim resulted.

Regulatory Proceedings Coverage

This would cover defense and fines and penalties in connection with a covered data breach, as well as failure by the insured to administer an identity theft prevention program required by regulators.

Lawsuit Coverage

The negative publicity that often surrounds a data breach can spur multiple complaints against financial institutions of all sizes. Plaintiffs' lawyers will exploit existing privacy laws and file complaints seeking huge damages, which can cripple an organization without insurance coverage.

Programing Errors & Omissions Coverage

This will pay for defense and damages for an insured when a programing error results in a wrongful act that results in the disclosure of PII from the insured's computer system.

Payment Card Industry (PCI) Fines Coverage

This comes into play when a covered breach event triggers fines and penalties for non-compliance with PCI industry standards.

CRIME POLICIES

Most of the standard exclusions relate to fraud and theft, which are common exclusions in most liability policies. This has become very controversial over the last few years, as the scope of cyber insurance policies has shifted away from covering cyber-related socially engineered theft and related wire fraud — or what is referred to as false pretense theft (usually by email) or electronic crime coverage.

Carriers have not universally abandoned this crime coverage in their cyber insurance policies, but if they haven't abandoned it, in most cases they have sub-limited it to a lower dollar amount than the primary policy limits.

It has become clear that cyber policies primarily respond to stolen *data* and crime policies respond to stolen *money*. Yet significant confusion remains. Even with an understanding of this broad coverage difference, crime policies can be complicated and difficult to understand.

Realizing that socially engineered wire fraud coverage may appear to be part of a standard crime policy, one needs to be very careful to distinguish whose money is covered for theft — the insured client's money, or the insured client's *customers'* money. It's easy to confuse these terms, and misunderstandings have been prevalent for years.

Most of the major carriers will now endorse (for an additional premium) crime policies (including Form 14 Bonds) to cover socially engineered wire fraud of the insured customers' money. There are a few that include customer assets in the standard form, but this risk requires careful underwriting.

Lastly, be cognizant of sub-limits and stringent conditional requirements on the insured's internal controls in connection with false pretense wire fraud coverage, like double and triple checks by more than one source (phone/text), that, when followed, could nearly eliminate the need for the coverage.

Lastly, cyber insurance underwriting has not yet matured into a predictable market, making it critical that your insurance professional has an understanding of the many moving parts that are in constant flux. PC

Paul J. Smith, AIF, is Senior Vice President at Starkweather & Shepley Insurance Brokerage in Westwood. MA. He can be reached at PSmith@stsrshep.com.

EVEN AT THE LARGEST COMPANIES, FUMBLING THE FIRST STEPS OF A BREACH RESPONSE IS COMMON, IF NOT INEVITABLE.

PREECHAR BOWONKITWANCHAI / SHUTTERSTOCK.COM

Dollars, and Sense

The 2017 Cost of Data Breach Study conducted by the Ponemon Institute, LLC for IBM found four common-sense factors that contributed to lowering the cost of a data breach:

- Having an incident response plan and team in place
- Extensive use of data encryption
- Employee training
- Use of data loss prevention software