Cyber Liability Insurance: Who's on First?

Published on May 24, 2017

Andrew Fotopulos | Follow
President at Starkweather & Shepley Insurance Corp. of MA

Recently, insurance coverage for various types of cyber liability has begun to be offered in the insurance market. However, there is still quite a bit of confusion surrounding what types of exposures are covered under cyber insurance, leaving many asking 'Who's on first?' This article addresses some common types of cyber liability exposures and claims, as well as some of the more salient coverage and cost issues that firms contemplating this type of insurance may want to consider.

E-mail Funds Transfer Fraud

One type of liability often asked about is e-mail funds transfer fraud. This type of loss requires a separate insurance policy, that is, separate from a "standard" cyber liability policy, thus adding to the confusion. E-mail funds transfer fraud is where a perpetrator sends an e-mail that appears to be from a client of a financial advisor requesting that the client's funds be transferred from one custodian or bank account to another custodian or bank account which turns out to be controlled by or accessible to the perpetrator. This type of fraudulent e-mail request is considered a "social engineering" attack and may be covered under a Fidelity Bond, assuming that the correct coverage rider has been attached. However, if it is actually funds of the insured firm -- not the client's – that is lost, then coverage falls under a cyber liability policy. Confusing, right?

Ransomware

Ransomware is another scenario that can give rise to cyber liability claims and is perhaps the most common type of cyberattack. Ransomware involves hijacking the

network is encrypted by the perpetrator and payment/ransom to "unencrypt" the data is demanded. The attack perpetrated against Sony Pictures in 2014 is one of the more famous cases involving ransomware.

Ransomware claims are covered under virtually all cyber policies. Although ransoms are typically for small dollar amounts, failure after the fact to detect the entry point will leave the firm exposed to repeat attacks.

The loss prevention services provided by cyber liability insurers may be, in many cases, well worth the premium. The good news is, as stated, ransomware attacks are covered under most cyber liability insurance policies. The bad news is that the firm must make sure that if the policy does have this coverage, there is no restriction that states disclosing to the perpetrator the existence of insurance to cover this loss may preclude coverage. As the saying goes, the devil is in the details.

Other Types of Claims

Other types of cyber liability claims may involve:

Claims for violation of intellectual property rights or unfair trade practices arising from a terms or phrases displayed on the insured's website or social media pages.

Claims arising from tax forms containing personal information being sent to the incorrect fax numbers.

Similarly, claims could arise if a custodian sends one customer's account numbers or holdings to the wrong customer.

Every day, it seems, new scenarios come to light that could give rise to potential cyber liability claims.

Coverage Issues

Every cyber liability policy is different and firms should be aware of the differences before making a purchase decision. The insurance broker selling the policy needs to understand the firm's business to make sure they are not selling a size 7 shoe to fit a size 9 foot. The result may be more than uncomfortable.

Here are some of the coverage issues to consider when reviewing policies:

1. *A retroactive date or prior acts exclusion.* A firm may have been in business for several years but purchases a cyber policy that applies only to events that caused a loss on or after the effective date of the insurance policy, leaving losses arising from prior acts uncovered. This is similar to the problem posed by a prior acts exclusion in a standard E&O (errors and omissions) policy.

restriction on ransomware coverage that prohibits disclosing the existence of insurance coverage.

3. *Limitations of the dollar pay out for notification of a breach based on a certain number of individual records.* Some insurance policies have a cap for the number of individuals to be notified, beyond which coverage is not provided. Keep in mind, the average cost of notification is around $200 per individual. If the notification is required to be sent to a number of individuals in excess of the cap, a significant gap in coverage can result.

4. *Short window of opportunity to report a claim.* Also, does the clock start ticking from when the incident first occurred or when it was discovered? If discovered, by who?

5. *A coverage exclusion for acts of "war" or "terrorism" with no carve backs for cyber terrorism.* It is very common for state actors to infiltrate cyber systems. Just ask Sony. If the attack is deemed to be an act of "war" or "terrorism," coverage might be denied.

6. *Exclusion for use of software with expired or withdrawn technical support.*Many software providers end support for their products frequently, pushing their customers to upgrade to their latest and greatest software. These exclusions might vitiate coverage for losses arising from software that the firm is slow in upgrading or chooses not to upgrade at all.

These are just a few of the items that could result in significant coverage gaps for any particular firm.

Trends and Developments

Some newer developments in cyber liability insurance include adding coverage to errors and omissions (E&O) liability insurance as an option to a stand-alone cyber liability policy. This is typically purchased at an additional premium cost. However, these options may offer more restrictive coverage and not always cover both first- and third-party losses. Also, these policies do not always come with the risk management tools of a stand-alone cyber liability policy. Included in those tools are both pre- and post-breach risk management resources, such as specimen written policies and procedures, employee training, pre-negotiated legal counsel, forensic and other professionals that assist with a breach response.

Another development when it comes to E&O as well as directors & officers (D&O) liability coverage is the tightening of policy language for failure to purchase, or the insurer does not offer, cyber liability extensions under the same policy. The insurers are making sure that their policy will not respond to any sort of cyber claim including those

identifiable information.

Getting Cyber Liability Insurance; Underwriting Considerations

Firms often want to know what they need to have or do in order to make them an acceptable risk to the insurance carrier or to help reduce the cost of cyber coverage. While each insurer will have its own underwriting considerations, most insurers will want to know that their customers have commercially available firewalls and anti-virus protection in place along with critical data being backed up on a regular basis. They will also want to ensure their customers have a formal process to disable or restrict access to information systems upon termination of an employee. There may also be coverage and premium advantages for firms that have personal information on portable devices encrypted, as well as being PCI-DSS compliant (that is, compliant with Payment Card Industry Data Security Standards).

The good news is, as stated, ransomware attacks are covered under most cyber liability insurance policies. The bad news is ....

Cost of Coverage

The pricing for cyber coverage varies among insurers and is typically based on different factors: revenues, number of records, number of employees and number of investment advisory professionals on staff are all possible premium determinants. However, with any of these rating categories there is something in common: the greater the number, the higher the cost. Policies with broad coverage provisions as well as policies with restrictive coverage may start as low as $1,100 in annual premiums for a one person small shop obtaining $1 million in coverage limits. In comparison, a firm with 10 or so investment advisory professionals may expect to pay closer to $3,700 annually for the same $1 million coverage limit. Of course, larger firms can expect even higher premium costs and will likely seek higher coverage limits.

Although premium cost is where many firms start their inquiry about cyber liability insurance, the cost of coverage should probably be a less prominent factor than it tends to be. Most firms drastically underestimate any risk and cost of a cyber event when deciding whether cyber insurance is affordable. In this regard, one thing seems highly likely: at the time of an event, the firm will not be at all concerned with whether it purchased the least expensive policy and, indeed, may have more significant regrets if it did not obtain the proper coverage or, worse yet, any coverage at all.

Conclusion

Cyber liability insurance is still relatively new. As a consequence, not much has standardized yet in terms of underwriting, coverage and cost, leaving many asking, "Who's on first?" However, the information in this article about exposures and claims,

of this type of insurance to the extent developed to date.

About the Author: Andrew J. Fotopulos, of Starkweather & Shepley Insurance Corporation of MA, is President, S&S Insurance Corporation of Massachusetts; Executive Vice President, S&S Insurance Brokerage Inc.; and Managing Director of the firm's Investment Industry Practice Group. He specializes in coverage design and risk management strategies for insuring financial institutions and their personnel, including investment advisers, securities brokers and dealers, mutual fund groups, private investment funds, hedge funds, Private Equity, Venture Cap, trust companies and banks.

Andrew Fotopulos
President at Starkweather & Shepley Insurance Corp. of MA
26 articles

1 comment Newest

Leave your thoughts here…

Yan Ross ··· 1w
Author of the Identity Theft Risk Management Textbook, Director of Special Projects, Institute of…

Read this thought-provoking article with much interest. One item missing from the underwriting section is employee education, since so many of the cyber-breaches occur as a direct or indirect result of the failure of employees to engage in healthy cyber hygiene practices and other risk management techniques usually falling under the rubric of identity theft prevention. Kn… See more

Like Reply

Don't miss more articles by Andrew Fotopulos