Protecting Against the High Cost of Cyberfraud

The Role of Cyber Liability Insurance in Your Risk Management Strategy

In a worst-case scenario, a massive cybercrime can be costly enough to bankrupt a business. Far more often, companies that are victimized survive but face enormous and costly consequences – including lost dollars, staff time expended to resolve the matter and a tarnished reputation with customers and the public.

Companies are discovering even when they take all the recommended precautions and incorporate sophisticated safeguards into their systems, there are no guarantees to avoid being hacked. Indeed, despite broad publicity about some very large breaches, cybercrime, for small and mid-sized companies, has been on a steady upswing.

Responding to this trend, many companies are finding cyber liability insurance can be an effective risk management tool. Today, a growing number of property and casualty carriers offer cyber risk policies at affordable rates. But given the relative newness of the coverage and the variability of policy features, it's essential to carefully analyze one's needs and scrutinize available coverage options before paying the first premium.

Paying the Price

Consider this: in 2016, the average cost of a data breach resulting from a successful cyberattack to a business has been estimated at $4 million.[1] Additionally, difficult to calculate – yet real – are losses stemming from reputational damage.

Other costs – beyond any actual loss of funds when fraudulent wire transfers are initiated – include those related to legal services, customer and employee communications, public relations, monitoring of customer credit, forensic analysis and, potentially, penalties from regulatory bodies.

A common type of cybercrime involves social engineering-based schemes to access corporate and customer data. These crimes occur when employees are deceived into believing they are interacting online with a colleague or company executive, then follow a link or open an attachment resulting in the release of information that allows cybercriminals to access and compromise corporate systems. The information fraudsters gain from these schemes is often used to transfer corporate funds to an unintended recipient.

On average, it costs

to resolve a data breach from a cyberattack

[1] "2016 Cost of a Data Breach Study: Global Analysis," IBM and Ponemon Institute, June 2016. Blog post and white paper available at: https://securityintelligence.com/media/2016-cost-data-breach-study/

McGriff | Insurance Services

Sylvia B. Menetre
Vice President, McGriff Insurance Services
SMenetre@McGriffInsurance.com • 678-537-8710

The Ransomware Scourge

Perhaps one of the most significant cyberthreats to companies today, as demonstrated by the massive "WannaCry" attack in early May 2017 and a subsequent similar attack originating from the Ukraine in late June 2017, is ransomware. The U.S. government estimates 4,000 ransomware attacks happen every day.[2]

In a successful ransomware attack, company systems are locked down by cybercriminals, and they are only unlocked after a ransom payment is tendered, typically in the form of an untraceable cryptocurrency like Bitcoin. Demanded ransom ranges from hundreds to thousands of dollars. The ransom payment may represent only a small part of the cost to the company, however.

The WannaCry event affected more than 200,000 computers in 150 countries and represented "a seminal moment in the development of the cyber insurance market," according to a report in the *Financial Times*.[3] Current annual premium revenue for cyber insurance is in the $3 billion to $4 billion range, but it is expected to reach $20 billion by 2025, according to the report.

Policy Provisions

"Network security and privacy" is the general heading for policies that cover cyberattacks. Although these policies vary, the following are the most common coverage areas in a comprehensive policy:

- ***Third-party liability:*** This includes the cost of defending against litigation initiated by customers and employees claiming they have been damaged by the attack.

[2] "How to Protect Your Networks from Ransomware," a U.S. government interagency technical guidance document. Available for download at: https://www.justice.gov/criminal-ccips/file/872771/download

[3] "Cyber insurance market expected to grow after WannaCry attack," Financial Times, May 16, 2017.

Evaluating a Cyber Policy

Here are some questions you should ask before purchasing any cyber liability policy:

- What prebreach services are provided by the carrier? Examples include risk assessments, mobile security apps, employee training, and risk management policy and procedure templates.
- What is the extent of business interruption coverage? Is there an extension for dependent business interruption?
- Does the policy cover reputational damage?
- For purposes of paying a ransomware demand, in the policy is "currency" defined to include cryptocurrency such as Bitcoin?
- Does it cover social-engineering, phishing scams where an employee is tricked into voluntarily parting with money through a wire transfer?
- What are the response and remediation processes following a breach? Are claims services in-house with a carrier-assigned breach coach, or are all services outsourced?
- Can you use your own attorneys to address the legal aftermath of a breach and then seek reimbursement, or are you required to use attorneys contracted by the carrier?

- ***First-party (i.e., the insured) basic expenses:*** Examples include hiring cyber forensic experts to investigate and fix the source of the breach, along with the cost of notifying all impacted parties.
- ***Additional first-party expenses:*** Data restoration expenses, lost revenue due to business interruption and costs related to external public relations services.
- ***Extortion payment:*** In ransomware attacks, it is often necessary to pay the ransom, while at the same time identifying and minimizing or eliminating the vulnerability that led to the successful attack.
- ***Liability for website content:*** A variety of liabilities arise from having a company website, including potential theft of proprietary content. Other liability can stem from copyright and trademark infringement.
- ***Health Insurance Portability and Accountability Act (HIPAA) defense and penalties:*** Exposure of protected private health care data, whether belonging to employees or others (in the case of a health care provider or insurer) can have costly consequences.
- ***Payment Card Industry Data Security Standard (PCI DSS) penalties:*** Such costs can be incurred if procedures for processing customer credit and debit card payments don't satisfy PCI DSS requirements and cardholder accounts are compromised.
- ***Extension for privacy in paper files:*** Although hard copy files are not subject to cyberattacks, their theft can lead to similar consequences as the exposure of some electronic files. Therefore coverage related to this risk is also typically found in the same network security and privacy contracts.

Policies with these features are not to be confused with small business owners' policies that include an extension for first-party breach expenses. Such policies are far more limited in scope and have low coverage limits.

Full-scope cyber policies are generally handled by carriers' professional lines departments and not folded into standard property and casualty (P&C) policies. However, in some situations premium savings might be available through combining the aggregate liability limit on a cyber policy with your errors and omissions (E&O) coverage.

Management Liability

Cyber policies can also be added to a management liability policy, but without sharing the aggregate limit. In addition, some directors and officers (D&O) policies shield those individuals from liability associated with cybercrime, and some do not.

The cost of comprehensive cyber policies is generally competitive in today's market, with many new insurance carriers regularly entering the market as demand grows. Cyber policy premiums as a portion of a typical company's total P&C coverage expense will be small. However, costs vary not only by industry sector and "record count exposure" – the number of personally identifiable information (PII) files in corporate systems.

The cost of comprehensive cyber policies is generally competitive … with many new carriers entering the market as demand grows.

Because the price of cyber policies is generally attractive in today's market, self-insuring, or retaining a significant amount of risk, might not confer any significant financial benefit. However, the larger the contract, the more worthwhile it is to at least consider risk retention levels in discussions with your insurance broker.

Incident Reporting and Safety Systems

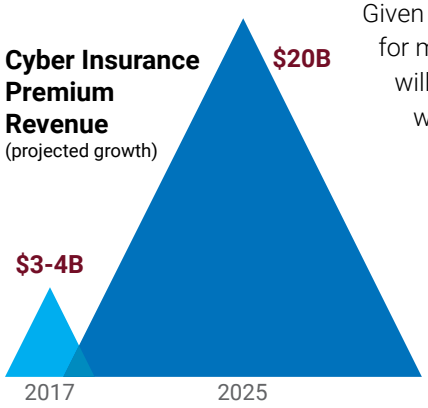
Cyber insurance policies are generally issued on a claims-made basis. The policy will require all circumstances that could give rise to a claim be reported before expiration of the policy term. If the carrier is not notified, and through the discovery process the carrier determines you were aware of a breach and could have brought in the carrier earlier to limit and remediate any losses before they grew, the carrier can deny a claim.

As with other kinds of liability insurance, the availability of coverage may depend upon, or be priced on the basis of, safety systems you put in place. Some insurance carriers, for example, might require full encryption on all company devices or any that access corporate systems, including laptops and smartphones.

A detailed application will be required for an insurance carrier to underwrite your risk. This application will include specific questions on your data security processes, encryption and vendor management to name a few. An exception exists for most small businesses under $10 million in revenue where only a minimal amount of underwriting data is required to bind coverage, subject to a no-claims warranty statement. Do not let the challenge of completing the application or the concern of not being adequately secure keep you from considering this critically important coverage. This is a competitive market and most applicants will receive a reasonable coverage proposal. There might be a few subjective carrier recommendations but that will only improve your risk profile moving forward.

Along similar lines, if you sustain a costly cyberattack and large claims are paid, at renewal time you might expect a premium increase or even a decision not to renew the policy. The measures you take in response to an incident to reduce the likelihood of future breaches will influence the decision to renew and any premium adjustments.

Taking the steps to be insurable and to secure appropriate insurance protection is more critical than ever.



Given the accelerating growth of cybercrime, for most companies it's not a matter of if they will be the target of a successful attack but when. Taking the steps to be insurable and to secure appropriate insurance protection is more critical than ever. The daunting variety and complexity of cyber policies can be overcome by working with an experienced broker with expertise in this rapidly evolving field.