CYBER INSURANCE: A GROWING IMPERATIVE

WHAT IT IS AND WHY YOU SHOULD CONSIDER IT
EXECUTIVE SUMMARY

CYBER CRIME IS A GROWTH INDUSTRY. THE RETURNS ARE HIGH AND THE RISKS TO THE CRIMINALS ARE LOW. ONE SURVEY ESTIMATED THAT IN 2014 ALONE, 81% OF LARGE COMPANIES AND 60% OF SMALL ONES SUFFERED A CYBER BREACH.¹ IN 2015, 38% MORE SECURITY INCIDENTS WERE DETECTED THAN IN 2014, AND THEFT OF INTELLECTUAL PROPERTY INCREASED BY 56% IN 2015.² THE AVERAGE DAMAGES PER INCIDENT WAS AS HIGH AS $5.9 MILLION FOR LARGE BUSINESSES AND $410,000 FOR SMALL ONES.³

Historically, many organizations believed that their existing insurance policies — general liability, commercial property or business interruption, among others — would cover them in case of a cyber breach. This is often no longer the case. A key turning point in public perception came after a recent high-profile cyber attack on a major media company. The firm’s general liability underwriter went to court and successfully got a preemptive ruling establishing that the breach was not a covered incident. This proved to be a wake-up call for many businesses.

Separate cyber insurance can specifically cover the damages and costs incurred as a result of cyber breaches. Although only a small fraction of companies today have such insurance, this is changing, and experts expect demand for cyber insurance to accelerate in coming years.

Cyber insurance offers many benefits. It provides financial resiliency in case of a serious breach. It improves your public security stance. And it streamlines contracting with other companies when sensitive information is involved.

However, the processes of securing a cyber insurance policy, filing claims and renewing your policy — an annual requirement — are complex and fraught with pitfalls. To successfully navigate these challenges often requires organizations to seek expert help.

Cyber insurance alone is not enough to protect you, of course. It certainly doesn’t replace your current portfolio of security products, services and processes. Instead, cyber insurance should be considered an important part of every company’s overall security strategy.

Going through the exercise of getting cyber insurance is valuable in and of itself. It forces you to have important conversations with all the relevant stakeholders in your organization about your overall cyber risk stance, your cyber threat profile and your current IT security posture. You can then decide, given all this, what your risks are, how much risk you can take on and what risk you want to pass on to an insurance company.

Cyber insurance should be considered an important part of every company’s overall security strategy.
THE NEED FOR CYBER INSURANCE

Cyber crime numbers are so bad, we’ve become desensitized. One study estimated that the cost to the global economy from cyber crime is likely more than $400 billion annually.⁴ A more conservative estimate would put the losses at $375 billion, but in reality they could be as much as $575 billion.⁵ This is serious: Even the lowest number named in the study is more than the total gross domestic product of many countries.

And the threat is growing. PricewaterhouseCoopers identified a 38% increase in detected information security events between 2014 and 2015, causing its Global Risk Consulting Leader Dennis Chesley to declare that cyber is “the risk that will define our generation.”⁶

Yet despite the fact that 73% of companies place cyber risk as a top-10 business risk, they often dramatically underestimate the real risks and costs of cyber crime.⁷

For example, Ponemon Institute found the average financial loss due to a cyber incident was $5.9 million for large companies, $1.3 million for medium-sized companies and $410,000 for small companies.⁸ And experts from security firm Mandiant, a FireEye company, estimate that the cost of several high-profile retail breaches in 2014 ultimately exceeded $1 billion each. All told, more than 100,000 security incidents per day hit companies around the world in 2014.⁹

AVERAGE FINANCIAL LOSSES DUE TO SECURITY INCIDENTS, 2013-2014

Figure 1: Cyber incidents more costly for larger organizations.
Source: Managing cyber risks in an interconnected world: Key findings from the Global State of Information Security Survey, 2015, PwC

---

5 Ibid.
8 Ibid.
Some businesses are keenly aware of these risks. A full 71% of insurance CEOs, 79% of banking CEOs and 61% of business leaders across all industries see cyber attacks as a threat to growth, ranking them higher than shifts in consumer behavior, the speed of technological change and supply chain disruption.\(^\text{10}\) More than half (52%) of companies believe their exposure to cyber risk will increase over the next 24 months.\(^\text{11}\)

Despite this risk, only 19% of companies have cyber insurance.\(^\text{12}\) And even the ones that are covered are underinsured. Ponemon Institute found that only 12% of the total costs of a typical cyber breach are covered by insurance.\(^\text{13}\)

That appears to be changing. As businesses wake up to the need to reduce their risk, the experts expect the global cyber insurance market to grow from $2.5 billion today to $5 billion in annual premiums by 2018 and at least $7.5 billion by the end of the decade.\(^\text{14}\)

In this white paper, we establish the need for cyber insurance. To do this, we first define what it is. We then explain the cyber insurance lifecycle, and walk through the process of buying a policy from an underwriter. We look at best practices and potential pitfalls of acquiring cyber insurance, and explain how engaging a third-party security firm to help can facilitate the process.

Above all, we stress that cyber insurance should be an active consideration of your overall security strategy. It does not replace your security mechanisms — your firewalls, your intrusion detection systems or your intelligence gathering. Rather, it provides you with increased financial resiliency in case of a major breach and documents your effort to address cyber risk issues while protecting your company against threats.

As businesses wake up to the need to reduce their risk, the experts expect the global cyber insurance market to grow to at least $7.5 billion by the end of the decade.

**CYBER INSURANCE DEFINED**

Cyber insurance is a very young industry — only about 20 years old — and its products and services are still being defined.

Fundamentally, cyber insurance is an insurance product used to protect businesses from Internet-based risks and, more generally, from risks related to information technology infrastructure and activities.

Covered losses today fall into two categories. First-party losses are the direct losses accruing to the firm that got breached. Third-party losses are the costs suffered by related third parties — customers or partners — as a result of a cyber breach.

\(^{10}\) PricewaterhouseCoopers. Insurance 2020 & beyond: Reaping the dividends of cyber resilience. 2014.  
\(^{12}\) Ibid.  
\(^{13}\) Ibid.  
Partial list of commonly covered incidents

- **Forensics:** This is the cost of investigating and analyzing an attack, often done by a third party with specialized expertise.
- **Notification expense:** In many cases, a breached entity will be required by law to notify customers, partners or suppliers who have been impacted by a breach. Even if this isn’t a legal requirement, many firms do this to help manage their brand and business relationships during and after a breach.
- **Public relations:** Depending on the size of a breach, extensive communications with the press and the business community might be required.
- **Business interruption:** If systems or data are unavailable due to an attack, and business is disrupted, this can be covered. This is generally the highest expense — in 2014 organizations suffered an average of $204 million in business interruption costs due to cyber attacks.\(^\text{15}\)
- **Credit monitoring:** It is becoming standard for companies that have been breached to offer consumers credit-monitoring services to protect them from any subsequent identity threat or financial fraud.
- **Breach coaching:** A breach coach is a high-level response coordinator, working with technical experts to isolate affected data, notify customers, retain necessary forensics professionals and manage crisis communications. A breach coach is often the first responder to an incident and helps the company triage the response to a breach.
- **Legal costs:** These can be hefty, as lawsuits filed against breached companies only add to all the business losses. Hiring legal experts and settling the lawsuits can add up to tens of millions of dollars.
- **Regulatory fines:** If any violations of regulations such as the Health Information Portability and Accountability Act (HIPAA) or Payment Card Industry (PCI) rules occurs, your organization may be fined.

You should also know what’s not covered. Theft of intellectual property, for example, is not currently insurable. Neither is the remediation of a breach. And much ambiguity still exists as to what cyber insurance should and shouldn’t cover because the industry hasn’t standardized its product offerings.

To understand what is covered in any given policy you should commit to memory the first three rules of insurance: read the policy, read the policy and read the policy. Prior to committing to coverage you should walk through the insuring clauses with your broker, underwriter and independent coverage counsel. That will help you avoid costly and unpleasant surprises and help you clearly understand how the insurer will respond if and when the policy is triggered.

---

CYBER INSURANCE PROCESS

The process of getting cyber insurance is superficially similar to procuring other types of insurance. The cyber insurance lifecycle has three stages: placing a policy with an underwriter, submitting claims and renewing the policy.

• **Buying a policy:** You complete an application that will ask questions about your current security stance: What protections do you have in place? How vulnerable are you? Are you in an industry that is being targeted by cyber criminals? Your insurance broker then presents your application to underwriters, who bid for your business. You go through an interview with your chosen underwriter, who delves deeper into your security stance to assess your risk profile. You then negotiate your policy terms: the premium, limits and sub-limits, deductibles and exclusions.

• **Submitting claims:** When you suffer a loss you submit a claim, just as with any other type of insurance. Depending on the limits and sub-limits of the policy you negotiated, you get reimbursed for insured losses as defined by your policy.

• **Renewing the policy:** After an annual re-evaluation of your risk profile and the general risk climate of your industry, your underwriter will offer you a new policy. If this new policy is unsatisfactory, you may begin the process all over again with another insurer. Your risk profile can vary substantially from year to year based on threat actors in play in your industry and your company’s or industry’s loss experience. For example, premiums for retailers skyrocketed in 2015 due to the volume of losses and the criminal activity in that sector.

A closer look at the placement process

The placement process is the most critical and complicated aspect of the cyber insurance lifecycle.

The role of a broker

The insurance broker is very important to the cyber insurance placement process. A broker does three basic things. First, your broker helps you document your current security posture along with its strengths and weaknesses. The broker then helps you with your application and your interview to present you to the underwriters in the best light. Finally, your broker helps you choose an underwriter and negotiates the fairest policy for you.

The role of the underwriter

Currently, more than 50 underwriters offer cyber insurance coverage. Some are new to the marketplace, while others have been offering coverage for two decades. A few of the top underwriters are Ace, Beazley, AIG and Zurich. The underwriter analyzes your risk profile and offers to provide insurance coverage for agreed exposures for a certain annual premium. Because of the newness of the cyber insurance market and lack of standard products and terms, the process of choosing an underwriter is about comparing not only price and features, but also the nature and quality of the underwriter relationship.
The application
You will be asked to fill out an application that asks about your current security profile. Cyber insurance application practices are limited; they typically ask traditional security questions about antivirus software, firewalls and intrusion protection and detection systems. But traditional security approaches no longer work against today’s advanced attackers. To the extent you perceive that the application doesn’t adequately communicate your actual IT security practices, give your broker the information and insights they need to present you in the best light to the underwriters.

The interview
After the application has been presented to the insurance companies, the insurance underwriters bid on the business. As part of the bid, they will generally want to interview you for more information. During the interview, you will have the opportunity to present a more complete portrait of your cyber security stance than you could in the application.

Keep in mind that underwriters are competing for your business. The underwriters will compete aggressively, but their approaches and appetite for your risk can and will vary. One underwriter might want a security program assessment while another will be content to interview your chief information security officer (CISO) and other stakeholders.

Policy components
It is critical to understand the various components of a cyber insurance policy and how they relate to one another. Adjusting your liability limits and sub-limits can impact your premium, as can raising or lowering your deductible. Off-the-shelf coverage is just a starting point. You should work with your broker to get the optimal mix of components. The goal is to get a fair policy at a fair price that responds the way you expect it to in the event of an insured loss event.

• Premium: This is the annual price for a cyber insurance policy. Premiums are determined based on a number of interrelated factors. Working with your broker, you can solicit multiple quotes to determine where the best value is being offered.

• Liability limits and sub-limits: Like other types of insurance, your cyber insurance policy limits what your underwriter will pay out in case of a breach. Whether that amount is $1 million, $50 million or even higher depends on how much risk you feel your organization can bear. However, you need to be especially careful about sub-limits: specific limits for specific losses. For example, you may have a policy with a $1 million limit, but a $50,000 sub-limit for notification costs. This could be a problem in a major breach, when notifications cost an average of $173,000.6 To set the correct limits and sub-limits, you need to thoroughly understand the current threat landscape as well as your current security stance. Hiring a third-party security company to perform a risk assessment is highly advised.

• Deductibles: The deductible is how much you have to pay toward your breach costs before you get payment from the underwriter. Be mindful that deductibles can be stated as time- or dollar-based, and you should understand the implications of each.

• Policy language: There is no standard policy language as it relates to cyber risk. Therefore it’s important that you clearly understand the insuring clauses in the policy.
BEST PRACTICES FOR OBTAINING CYBER INSURANCE

Here are some best practices you should follow when placing a cyber insurance policy.

**Be sure your security investments and cyber insurance complement each other**

The decision to buy insurance is a question of risk tolerance. Publicly traded entities in particular are under greater security scrutiny. While not every company will need cyber insurance, every company should evaluate and document how the decision to obtain or decline insurance was made.

Remember, you can invest in security without insurance, but you won’t be able to procure large limits of insurance without demonstrating to the underwriter that your company engages in reasonable security (otherwise, underwriters will determine that your risk profile is too great to warrant issuing a policy). Irrespective of the maturity of your security posture, you should go through the cyber insurance placement process as a valuable exercise in assessing your risk profile and risk tolerance.

**Engage a knowledgeable broker**

Engage a broker who is cyber savvy and understands cyber risk and how the insurance market is currently assessing different levels of cyber risk. A good broker will walk you through the application process and make the best case for you to underwriters.

**Go beyond the application form**

Your goal at all times in the placement process is to demonstrate a strong security posture that demonstrates an ability to minimize risk and provides the underwriter with a clear picture of the risk you face.

This often means going beyond the application form. Recognize that the application is just a starting point. Answer the questions asked, but as an internal exercise also answer the questions not asked. You want to be able to provide sufficient risk clarity to help ensure you are getting the coverage desired at a fair price. To achieve this, put in the time and effort to be clear about your security posture. Incorporate your use of intelligence, real-time or otherwise, and your ability to respond to losses either in-house or through retained third parties.

**Focus on a “fair” price rather than a “best” price**

You have multiple levers to pull in the conversation about limits, sub-limits, deductibles and time periods and how they all relate to premiums. Although getting the “best price” may be an easy way to measure success, it’s impossible to know what that price actually is in a cyber insurance market that lacks uniformity or maturity. Therefore your goal should be to secure the most useful coverage at a fair price.

Specifically call out if you retain a third party to provide threat intelligence or incident response services. The existence of an agreement with a top-tier vendor will benefit both your company and the underwriter and can help as you negotiate the various components of the policy.
Engage experienced outside counsel to review insurance terms
An insurance policy is a legal contract. It is imperative that you engage experienced outside counsel to review the insuring clauses and point out areas of additional consideration.

Specifically, you’ll want legal counsel experienced in cyber insurance to read through the policy and make sure that you fully understand all the provisions, and that it makes sense for your organization.

Engage cyber security experts
It’s a fact: the more effort you put into the process of securing an insurance policy, the more likely that liability limits, deductibles and policy language will benefit you. A third-party security company or consultant working with your broker can help you navigate the process.

Even before filling out the application, you may want to engage a cyber security firm to perform various assessments. These assessments will work for you in three ways. First, they’ll show you your current vulnerabilities, and how to strengthen your security stance. Second, they’ll document your current state of response readiness; this will help the broker present your business in the best light and help the underwriter assess your risk level as a potential customer. Finally, security assessments can also help you estimate how much coverage you need and what the limits and sub-limits should be.
Independent consultants can also provide several types of risk assessments:

- **Security program assessment:** A third party conducts an in-depth analysis of your security structure and helps you create an action plan to strengthen it.

- **Compromise assessment:** A third party performs a detailed review of your systems to determine if you are currently under attack or have previously experienced a cyber breach.

- **Response readiness assessment:** The third party assesses your ability to respond effectively in case of an attack.

- **Health checks:** The third party provides an in-depth, individualized look at your risks using technology, intelligence and expertise to analyze your network traffic, files and endpoint activity.

Any of these assessments can be used to help present a strong risk profile to an underwriter.

**CONCLUSION: NOT A COOKIE-CUTTER APPROACH**

No company can be 100% secure. There are unforeseen threats and fraud schemes that the best-designed internal controls cannot prevent. Therefore, insurance needs to be considered a part of every company’s active security strategy. This consideration should include input from all the key stakeholders in the enterprise including risk management, the chief financial officer, IT leadership, legal experts and the board.

The trend towards securing cyber insurance is undeniable. But the best approach to securing useful insurance is not a cookie-cutter approach. Each company should go through a considered process to secure coverage that will address the most likely cyber risks they face.
HOW FIREEYE CAN HELP

FireEye is not a broker or underwriter, but we are focused on providing capabilities that enhance the role of insurance. Our goals are to update and inform the insurance community on how best to address and manage cyber risk. This streamlines the underwriting and claims process so that our clients who experience a breach can be more resilient in both their operational and financial recovery.

Underwriters should understand a potential insured’s ability to prevent attacks from occurring, but they also need to take it a step further and assess the insured’s ability to detect, analyze and respond to exposures to minimize losses. FireEye is investing time and effort with the insurance community to upgrade this approach. Our products and services are entirely complementary to organizational insurance programs, provided the underwriter recognizes the value that FireEye clients gain by working with us.

FireEye works directly with the insurance community to develop capabilities to promote the adoption and implementation of fair cyber insurance for our clients.

ABOUT FIREEYE

FireEye protects the most valuable assets in the world from those who have them in their sights. Our combination of technology, intelligence, and expertise — reinforced with the most aggressive incident response team — helps eliminate the impact of security breaches. We find and stop attackers at every stage of an incursion. With FireEye, you’ll detect attacks as they happen. You’ll understand the risk these attacks pose to your most valued assets. And you’ll have the resources to quickly respond and resolve security incidents. FireEye has over 4,000 customers across 67 countries, including more than 650 of the Forbes Global 2000.
To learn more about how FireEye can help you with cyber insurance, visit: