

Cyber insurance

Despite an appeals court ruling, experts still recommend buying cyberinsurance. But, not all policies are the same.

ebook

An SC Magazine publication

Sponsored by



SECUREAUTH

Insuring security

Cyberinsurance has been booming in recent years as organizations face growing concerns about the cost of online breaches. But confusion still abounds about what these policies cover that basic business insurance, or other policies, do not. **Karen Epper Hoffman** reports.

In recent years, companies have turned increasingly from a cybersecurity stance of “protecting the perimeter” to accepting that when it comes to being breached, it is likely more a question of *when* rather than *if*.

With that heady realization, and all the high-profile online attacks that have made headlines in the consumer and business press, more organizations than ever before are taking significant steps to protect themselves in the almost-inevitable event of being hacked. And, for an increasing number of organizations, one major step has been to invest in a cyberinsurance policy, designed to help offset the often exorbitant costs an online corporate breach can entail.

However, legal decisions and the overall maturing of this fast-rising segment of the market are causing many industry insiders to question what these policies really cover. Given a recent case at the U.S. Court of Appeals for the Fourth Circuit in Virginia that ruled general business insurance addresses cyber breaches, companies are beginning to question whether separate cyberinsurance is even necessary.

“There are many misconceptions

among all of the parties involved,” says Craig Shumard, principal for Shumard and Associates, a strategic security consulting firm, and former CISO for Cigna. “Buyers sometimes have an unrealistic expectation of what activity is covered and what is not covered. Probably the biggest misconception is that insurance will allow for reduced spending and less mature security programs.”

Michael Molinaro, CISO of BioReference Laboratories, says policy buyers generally operate on the premise that cyberinsurance covers the entire breach lifecycle and expense. “Unfortunately, this is not the case,” he says. “Security events, incidents and breaches are different issues.” Companies experience security incidents as part of the normal business operations, while breaches imply information was “exfiltrated and accessed by unauthorized parties,” he says.

Indeed, while cyberinsurance has been around for at least 15 years, it has only been in the past few years – in the face of breach damages running into eight- and nine-figure costs and hitting the headlines more frequently – that many organizations have been buying these policies. Buoyed by these concerns, the cyberinsurance market is expected to triple

to \$7.5 billion in annual premiums between 2015 and 2020, according to research from PwC. While 90 percent of cyberinsurance policies are currently purchased by U.S. enterprises, only one-third of companies here already have cyber coverage – making it a fairly nascent market with lots of room for growth. However, the PwC study also found the high cost of these

OUR EXPERTS: Cyberinsurance

Roota Almeida, head of information security,
Delta Dental of New Jersey

Yong-Gon Chon, CEO, Cyber Risk Management

Stephen Cobb, security researcher, ESET

Alex M. Hageli, director for the personal lines policy,
Property Casualty Insurers Association of America

Tatiana Melnik, attorney, Melnik Legal

Michael Molinaro, CISO, BioReference
Laboratories

Lysa Myers, security researcher, ESET

Jeff Recor, principal of risk advisory services,
Grant Thornton

Craig Shumard, principal, Shumard & Associates

Mike Spanbauer, vice president of security, test
and advisory, NSS Labs

Cyberinsurance

>70%

Percentage of
companies that report
being successfully
breached by a cyber-
attack in the past year.

– NetIQ 2015 Cyber-
threat Defense Report

premiums and the often restrictive conditions laid out in the policies limit greater growth.

“The cyberinsurance business is one of the fastest growing areas in the insurance sector based on demand,” says Yong-Gon Chon, CEO of Cyber Risk Management. The majority of buyers of cyberinsurance have been from the United States, but he says that “the EU market has significantly grown due to ever-increasing data breaches.”

Policy buyers, as well as mid-size and smaller brokers, are relatively uneducated about clauses, such as coverage limitations or what’s considered cyber versus general liability, Chon adds.

Appeals court ruling

As a specialty offering, cyberinsurance typically differs from general liability in that those policies will often cover physical damage. But in the case of a system being hacked or a corporate system falling prey to a virus, general liability policies might or might not provide coverage.

The issues are often in question of where the general business policy ends and cyberinsurance picks up, and what types of incidents or events a particular cyberinsurance policy will cover, and what exceptions are made, say in the case of cyber terrorism or employee misconduct. Ultimately, these can vary widely based on the company, the sector, the insurance carrier and the specific policy. That, in part, is the wrench that the Appeals Court decision has thrown into the insurance industry mechanism as experts try to determine just what is and is not covered.

Tatiana Melnik, attorney for Melnik Legal in Tampa, Fla., maintains that despite concerns created by the court’s ruling, “cyber liability insurance is necessary even if organizations

already have general business insurance.”

While there are several ongoing cases throughout the United States that address the scope of coverage of commercial general liability policies, and while the Appeals Court ruled in favor of the insured, Melnik points out that other courts have not. “Going to court to fight over the scope of coverage should really be the option of last resort,” she says.

Additionally, she adds that in 2013 the International Organization for Standardization (ISO) released a series of data breach exclusions that “make it nearly impossible to obtain coverage for a data breach under the commercial general liability policy. Insurance regulators have adopted these exclusions and they are routinely included in carrier quotes,” she says.

Alex Hageli, director for the personal lines policy for the Property Casualty Insurers Association of America, an industry trade association, agreed that the court’s decision, like most coverage cases, “will have a pretty

limited impact, in that the question of coverage is always unique to the particular policy’s language and the circumstances of the claim.”

Courts sometimes impose coverage where none was intended, Hageli says, and, as a consequence, “insurers periodically fine-tune definitions to clarify what coverage is in fact intended and what would be excluded.”

Insurers are also expanding cyberinsurance

riders to provide more options to consumers as well, to make clearer what is covered under different policies, Hageli says. This increased clarity and specificity will make cyberinsurance more necessary for prospective policyholders, he says.

Stephen Cobb, security researcher for ESET, also believes this federal appeals court case hinged on “specific language being construed



Yong-Gon Chon, CEO, Cyber Risk Management

50%

Half of all cyber breaches between September 2009 and August 2015 were unauthorized access and disclosure.

– TriPoint Healthcare Solutions

to cover a specific type of breach. So, although the ruling was a good one for companies that have similar language in their current coverage and have to face a similar situation, it cannot be generalized to the point where companies can assume ‘we have cyber risk covered because we have general business insurance.’”

Instead of relying on general business insurance, Cobb maintains that would-be cyber-insured individuals need to push for a better understanding of cyberinsurance, particularly what it covers and what it does not, as well as where it overlaps with general business insurance. “What is necessary is that firms understand what coverage they are getting, whatever policy it comes through,” Cobb says. “At the moment, we don’t see comprehensive cyber risk coverage included in general business insurance.”

In general, Cobb says the maturing cyber-risk insurance market is a good thing because it is driving wider adoption and better implementation of standard security practices. “Issuers of these types of policy have a vested interest in helping clients improve their cyber defenses and responses to minimize incident frequency and impact,” he says.

While this is still a budding market, Chon believes the need for cyberinsurance still comes down to “understanding the fundamentals of an organization’s risk posture or risk appetite.” As an example, he says, imagine a Fortune 1000 company that has heavily invested in robust security, privacy, audit and analytics capabilities and understands how its data flows into and out of the organization, knows its users, its suppliers and third parties well, and maintains proper safeguards in place. Such a company might look at cyberinsurance as “mostly unnecessary. But also, the converse could be said to be true.” In other words, it

could be argued that the companies that are most cybersecurity-aware need cyber-specific insurance just as much as the companies that are not as prepared for an online threat.

“I think cyber will continue to evolve and will be a more standard insurance offering,” says Shumard. But, he adds, he is not sure whether the Appeals Court ruling in itself will change things.

Growing pains

“There are a couple of outstanding concerns with the cyber risk market, and they are the lack of actuarial data to support underwriting coverage and the lack of standardization of terminology,” says Hageli. “These are the same two issues, however, that arise anytime a new market develops and we are confident

that the market will address both issues.” Despite concerns, Hageli points out that the cyberinsurance market is growing at about 30 percent annually.

Melnik agrees that the availability of cyber liability insurance is increasing as more insurance companies are offering coverage, but she also raises concern around the use of off-site vendors and third parties. “Buyers need to be wary, particularly

if they are operating businesses with various staffing structures and have data stored at off-site locations controlled by vendors,” Melnik points out.

The insurance industry and underwriters are struggling to determine how to develop the required actuarial tables. They are building a framework based on breaches and are pricing cyber policies in a format that provides confidence in those products, according to Molinaro at BioReference Laboratories. “In essence, cyberinsurance is inconsistent and volatile due to a lack of long-term historical data,” he adds.



Tatiana Melnik, attorney, Melnik Legal

22%

Business associates are responsible for 22% of data breaches greater than 500 individuals.

– TriPoint Healthcare Solutions

“It is still difficult for cyberinsurance companies or the organizations themselves to properly assess cyber-risk,” says Roota Almeida, head of information security at Delta Dental of New Jersey. “With little relevant historical claims data, it is not easy to predict the likelihood of a claim being made, or to calculate the maximum probable loss,” she says. From a claims perspective, the ambiguous nature of the consequences of a data breach also makes accurate reserving difficult, she adds. The goal is to quantify cyber risk more accurately, as actuarial data is often scarce. An ideal form of cyber risk management requires a balance between IT security measures and transfer of risk as an insurance solution for cyber risk, she says.



**Roota Almeida, head of information security,
Delta Dental of New Jersey**

Almeida adds that insurers specialize in pricing and underwriting risk while cybersecurity experts specialize in managing security. “There is confusion regarding whether credit monitoring should be covered or if forensics investigation of the breach should be covered.” If some of this is covered, she asks, then to what extent? How is brand management going to be handled after the breach? Is that something that a cyberinsurance policy will cover? Will the cybersecurity solutions that an organization has put in place help reduce the premium? “All these questions are still points of confusion for an organization shopping for such a policy,” she says.

Lysa Myers, security researcher at ESET, agrees that in the face of this upheaval in the market, insurers and the insured are working together to find the best balance of coverage versus cost. “Both parties are realizing how common cyber incidents are, and how much an attack can directly affect a company’s bottom line. This means that more insurance companies are including cyber attacks in

their policies in one form or another.”

Estimates vary on how much cyberinsurance policies cost, but Myers says past policy

holders indicate it starts at around \$15,000 to \$20,000 in annual premiums for every \$1 million in coverage, which can increase based on the level of coverage and other factors. Depending on the sector, companies may have tens of millions of dollars’ worth of coverage, especially given the high cost of cleaning up and managing recent online breaches.

“There are important questions that are currently being addressed surround

exclusions and ‘due diligence,’” says Myers. “Such as, ‘What costs will not be covered? What is the minimum acceptable security level the insured must have in place?’”

A question of coverage

What can cyberinsurance cover? Does it include expenses related, but not limited to, crisis management during the incident and investigation or even through the potential legal issues that might follow? Other potential expenses could include online liability, such as rebuilding a defaced or damaged website; legal fees related to extortion; and customer and third-party damages related to denial of access or theft of information. The question, however, is often not what these policies *can* cover, but rather what they *will* cover.

Mike Spanbauer, vice president of security, test and advisory for NSS Labs, says there is also a fair amount of confusion on the insurer side “with respect to deciding how to price premiums in the face of little to no actuarial data.” But that’s not all.

“Policies vary wildly,” Spanbauer says. “It is not always clear to customers if separate cyber policies are required. They typically are.”

Policies that cover losses of customer data

\$100m

Recommended minimum cyberinsurance coverage for a large enterprise.

– Forrester report, 2014

are becoming more uniform, he says, and the policies usually cover costs of the basic forensic investigation of a breach, notification of clients



Losses that are the result of poor security practices or failure to disclose issues are not covered.”

– Craig Shumard, principal,
Shumard and Associates

that their information has been exposed, and credit monitoring services to those customers.

Molinaro says each insurance company has products that cover cyber breaches differently. “There doesn’t seem to be a standard or baseline. Interpretation is up to the actuarial and underwriter’s knowledge and perception when developing their products and services,” he adds.

Compounding confusion on the customer side, Molinaro says boards and C-suite executives are still not sure how to manage cyber risks in a vast majority of businesses. “Cybersecurity is the sexy topic in any company or conversation with business executives, however, funding and deploying a risk-managed cyber security defense plan is not feasible in most cases,” he says.

Delta Dental’s Almeida says that due to the large number of data breaches, cyberinsurance is necessary for organizations of all sizes and industries. “Even if a company is confident in its own IT controls, it might still be exposed to cyber risk through its business partners, contractors or supply chains. It’s not just about data loss or reputational damage, but business interruption due to a cyber breach could create havoc in organizations.”

For example, a major data breach or network

outage at a cloud service provider could cause business disruption for hundreds of companies. Awareness of risks due to business interruption is increasing and inclusion of that in a cyber-insurance policy could be a major selling factor.

According to Shumard, a former CISO, coverage and exclusions in cyberinsurance are often misunderstood, even by some brokers in the industry. For example, he says that intellectual property or trade secrets are very hard to underwrite and for the most part excluded, and most insurance companies will not cover the cost of so-called “reputational risk” because of limited expertise gauging this cost. In addition, Shumard says, “Losses that are the result of poor security practices or failure to disclose issues are not covered... and nation-state cyber actions are probably going to be excluded.”

Melnik agrees that the scope of coverage is the biggest point of confusion. “I’ve seen a number of situations where companies

purchased cyber liability coverage that provides very little to no coverage based on the way the company actually does businesses.” She says many policies still exclude coverage for data stored with third parties, which means any company using Office 365, Google Apps for Business, or another third party-managed system for email might not be covered in this area in the event of a breach. Meanwhile, she says some policies exclude

coverage for independent contractors when there is no written agreement in place, which means “companies that do not have robust contract management programs in place could be severely compromising the value of the insurance coverage with such an exclusion.”

Jeff Recor, principal of risk advisory services for Grant Thornton, says a lot of the confusion traces back to “the language of the policy,” which can lack clarity in many different types



Craig Shumard, principal, Shumard and Associates

Cyberinsurance

~90%

of companies
do not purchase
cyberinsurance.

– Chubb

of insurance policies. He maintains that larger insurance carriers with a history of providing cyberinsurance for a dozen years or more are less likely to be unclear in their coverage and exclusions. But issues still arise. Case in point: Cyberterrorism, particularly for international companies, often is still not covered. But what differentiates an organized and well-funded hacking ring operating overseas from a nation-state committing terrorism? This can be a point of contention.

Another major point emerges over the question of whether the organization did all that it could to protect itself and its assets effectively. ESET's Cobb says that when it comes to exploring and using cyberinsurance coverage "there is still no substitute for security best practices." According to a recent survey from NTT Com Security, respondents said their cyberinsurance

could be invalidated due to a number of issues, including a lack of compliance (48 percent), the age of their IT systems (39 percent), and lack of employee care or attention (37 percent).

"Insurance is a form of risk transfer, not responsibility transfer," Cobb points out. "A company that suffers a breach that exposes PII [personally identifiable information] will still be held accountable, regardless of the level of insurance coverage, but that coverage can offset the cost of dealing with that accountability."

But many policy holders and insurance industry carriers might ask: If the organization is not acting responsibly, will the coverage still be honored? And, an even bigger question is: What defines acting responsibly to mitigate cyber risk, when it is so inherent in most companies' day-to-day business?

"Right now the biggest point of contention seems to be what constitutes negligence on the part of the insured," Myers says. "It's a good

idea to be very clear about what is expected of you by your insurer before signing a policy." This can benefit those organizations that have good security practices since there are often cost savings for organizations that can prove they are taking proper precautions to identify and mitigate risks, Myers adds.

In the face of this confusion and concern, many organizations might still be on the fence about whether they even need

cyberinsurance, or whether their general business liability coverage would be sufficient. Indeed, this question was further bolstered by the Appeals Court case that ruled that general business insurance already addresses cyber breaches.

For now, Molinaro believes that despite the growth pains in the marketplace, having at least minimum liability for breaches can be analogous

to having the minimum comprehensive and property casualty car insurance. And products will improve as the market shakes out.

"The most common arguments in court cases are 'who was harmed?' and 'what are the damages?'" he says. As insurance companies understand the lifecycle and overall long-term effect of a breach, they can create different lines of business within cybersecurity products themselves in the same way that they have products for directors and officers or property-casualty policies, he says. ■



Jeff Recor, principal of risk advisory services, Grant Thornton

For more information about ebooks from SC Magazine, please contact Stephen Lawton, special projects editor, at stephen.lawton@haymarketmedia.com.

If your company is interested in sponsoring an ebook, please contact David Steifman, VP, publisher, at 646-638-6008, or via email at david.steifman@haymarketmedia.com.

32%

Average increase in cyberinsurance rates for the first half of 2015 after staying flat in 2014.

— Marsh



SECUREAUTH

SecureAuth was founded in 2005 with an innovative approach to solving user access control challenges, not just by adopting the latest technology, but by understanding the business problems causing them, and by taking a different approach to solve them. IT organizations are confounded by an ever-shifting landscape when it comes to access control with their application resources. In order to solve the unique challenges this presents, SecureAuth Corporation developed SecureAuth Identity Provider™ (IdP). This is a groundbreaking solution that turns any enterprise into an identity provider capable of enforcing two-factor authentication, adaptive authentication and single sign-on in a single, cost-effective solution.

For more information, visit www.secureauth.com

Sponsor

Masthead

EDITORIAL

VP, EDITORIAL Illena Armstrong
illena.armstrong@haymarketmedia.com

SPECIAL PROJECTS EDITOR Stephen Lawton
stephen.lawton@haymarketmedia.com

MANAGING EDITOR Greg Masters
greg.masters@haymarketmedia.com

DESIGN AND PRODUCTION

ART DIRECTOR Michael Strong
michael.strong@haymarketmedia.com

CUSTOM MANAGER Kelly Heismeyer
kelly.heismeyer@haymarketmedia.com

SALES

VP, PUBLISHER David Steifman
(646) 638-6008 david.steifman@haymarketmedia.com

EAST COAST SALES DIRECTOR Mike Shemesh
(646) 638-6016 mike.shemesh@haymarketmedia.com

WEST COAST SALES DIRECTOR Matthew Allington
(415) 346-6460 matthew.allington@haymarketmedia.com

HOW DO YOU KNOW YOUR USERS ARE WHO THEY SAY THEY ARE?

Billions of dollars have been spent on endpoint and network security and yet breaches still persist. That's because attackers disguised as valid users are using compromised credentials to access your network and applications. Progressive organizations are turning to SecureAuth for next-generation adaptive authentication solutions that strengthen security with the least amount of user friction possible - ensuring their users are indeed who they say they are.

Learn how SecureAuth helps determine identities with confidence at:
secureauth.com/determine-identities.

