A SPECIAL REPRINT FROM THE

NATIONAL UNDERWRITER

Property & Casualty / Risk & Benefits Management Edition

COVER STORY

Cyberinsurers, Producers: Opportunists or Saviors?

By **Peter R. Taffae**

Since the introduction of cyberinsurance products roughly three years ago, articles have been written questioning the insurance industry's approach to the new cyberspace exposures.

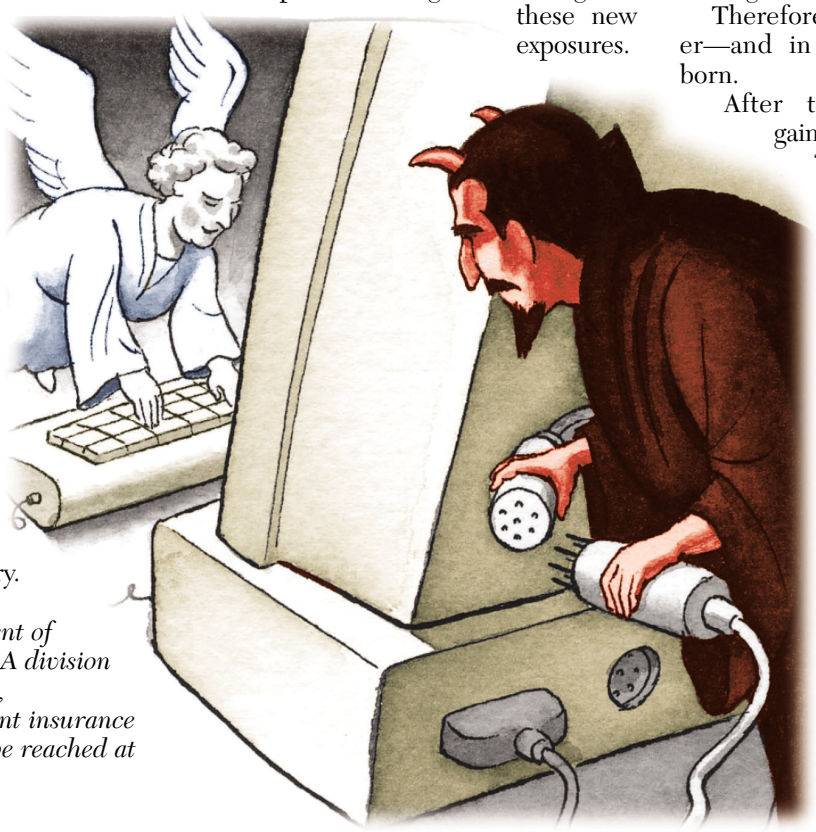
The critics of standalone cyberinsurance products usually build their arguments around two general themes.

• The first argument is that insurance companies (and I assume brokers, as well) are always looking for new ways to repackage existing coverage to collect more premium (and commissions).

• The second argument that these same critics make is that coverage provided under cyberinsurance policies already exists.

Therefore, in a nutshell, the insurance industry is made up of redundant money scavengers and opportunists.

I think both arguments not only underestimate the exposure, but they also underestimate the quality of individuals and companies in the insurance industry.



Peter R. Taffae is the president of e-perils.com in Los Angeles. A division of Worldwide Facilities, Inc., e-perils.com is an independent insurance wholesaler. Mr. Taffae may be reached at PeterT@eperils.com.

Let us address the contractual weaknesses of standard policies in order to address the arguments put forth against dedicated cyberinsurance programs.

Three-plus years ago, a few underwriters and brokers saw a coverage and expertise void in the marketplace. Once underwriters took the time to gain expertise and to understand the exposures that the new economy produced, they began to re-evaluate the products being offered in light of these new exposures.

They quickly realized what both the traditional property and liability underwriter fully understood—that existing policies were not designed for these new perils, such as viruses, hacker/cracker exposures, or denial-of-service attacks. The traditional underwriters who were offering standard policies (covering tangible perils, such as flood, fire, and wind) were not comprehensively underwriting these new perils.

Therefore, a new breed of underwriter—and in some cases, broker—was born.

After these "new" underwriters gained an appreciation for the "e-perils," they rightfully designed products that they felt allowed them to protect against cyberspace exposures.

Did they see this as a way to make money?

I am sure they did. I can tell you, however, that in the past year, not all of them made money on their cyberinsurance policies. As a matter of fact, a number have withdrawn from the market completely, because of the large losses that they have already sustained in this new segment of the insurance industry in the products' infancy.

Business interruption coverage provides one of

the most overt examples of how a traditional policy will not fulfill the unique needs of insureds conducting business on the Internet—or using other technologies, such as cellular. It would be hard, if not impossible, to find a well-informed individual that could intellectually argue that a denial of service to an insured using a business-to-business (B2B) or business-to-consumer (B2C) Internet-based business model results in "physical damage" to "tangible property." Yet this is a standard requirement of a traditional property (business interruption) policy.

There are other examples as well.

I will concede that a cyberliability (third-party liability) policy potentially has some overlap with a well-designed, comprehensive property-casualty program. I will also say, however, that there are cyberinsurance policies available that provide coverage that does not exist in standard policies.

I will not give in to those who argue that an insured that conducts business on the Internet would be fully protected without a dedicated cyberliability policy. There are clear advantages of cyberliability policies, such as contractual comprehensiveness and risk manageability.

Assuming there is coverage for certain perils elsewhere, I would suggest that it would be because the "standard" policy is "silent," not because the underwriter expressly intended to cover them.

Intellectual property rights, specifically trademark and copyright, are a major source of exposure in the World Wide Web. A quality cyberliability policy will protect the insured from infringement litigation. The comprehensive general liability is not intended to provide this coverage to an Internet company. The coverage under a CGL is for incidental advertising. I suggest that a Web site is not "incidental."

Because it was not the intent of the underwriter to cover such perils, courts are hearing (and will continue to hear) arguments over the nuances of contract language in standard policies.

To advise an insured to presume coverage under standard policy conditions is, in my opinion, misleading and ill advised. One could easily question the prudence of an agent or broker who chooses not to discuss a dedicated cyberinsurance product, in this new environment.

It is equally important to consider typical claims scenarios under one policy or numerous policies. What happens, for example, if an insured is an "e-broker"—a stock broker conducting business over the Internet—who falls victim to a major denial-of-service attack?

First, there is the business interruption loss—and we have already addressed the reasons why a standard property policy would not cover a denial-of-service attack claim that is submitted to the first-party underwriter.

Second, the e-broker's clients, who suffered financial losses resulting from their inability to access their accounts when the service was down, will likely bring lawsuits against the broker. Such lawsuits, which could have class action potential, would be sent to third-party underwriters. Whether or not a comprehensive general liability policy would cover this type of third-party loss is a legitimate question.

I would suggest that it would not, since the peril is not associated in any way with "bodily injury" or "property damage."

Under the correct cyberinsurance policy, the insured would only have to deal with one company—and that company would be one that has seen this type of claim before—rather than two companies that do not have individuals dedicated to handling these types of claims or the experience.

We see the majority of cyberinsurance policies being offered, not as attempts to "rake in more money selling the same box of soap twice." Instead, the professionals who have created them are willing to underwrite the new perils in dedicated, specific policies. They are hoping to be players in this new market for a long time and to earn the respect of brokers and insureds that recognize these new e-perils.

Finally, it is important to note that each insured is unique and that one approach will not be right for everyone. To truly determine whether "piggybacking" on existing policies is the best risk management strategy—or whether a specific cyberinsurance policy is a better alternative—the potential insured must first establish priorities and fully explore all options, evaluating the pros and cons of each approach. Only then can the insured make an intelligent decision.

If you are an agent or broker, be sure to seek expert advice on the constantly and rapidly changing products that are emerging in this area.