POLICY EVOLUTION

Eyes Wide Open

Eight things everyone should know about cyber insurance policies

By Peter R. Taffae

Less than two months ago, late in the afternoon of Jan. 19, the U.S. Department of Justice website vanished from the Internet. Anyone attempting to visit it to report a crime or submit a complaint received a message saying the site was unable to load.

More websites disappeared in rapid succession. The Recording Industry Association of America. The Motion Picture Association of America. Universal Music. Warner Brothers. The FBI.

By nightfall, most of the sites had come back online, but the people responsible for the outages had made their point. They'd landed what they hailed as the biggest blow yet in an escalating war for control of the Internet.

The World Wide Web is ever changing, with new sources of risks emerging daily that were impossible for us to imagine a decade-and-a-half ago. In many ways, the Web is still in its infancy, not only in terms of the level of sophistication of threats, but also with respect to the changing legislation and judicial decisions developing in response to the cyber frontier.

Simultaneously, the cyber insurance coverage market has blossomed in the 15 years since we brokered and co-wrote one the insurance industry's first cyber policies for a business-to-consumer company. At the time, four other insurance companies were getting into the cyber insurance business using an off-the-shelf miscellaneous errors and omissions policy and amending the "services provided" clause to name what at that time was thought to be an extensive list of perils. Although the list could be a full-page long, with exposures like meta-tag misuse and trademark infringement specifically identified, what it did—innocently—was to turn an all-risk coverage into a named perils form.

In the last decade, policies have broadened and the field of cyber underwriters has grown to over 20 players, with most offering both liability and prop-

erty coverage arising from cyber events. All the carriers have different underwriting approaches and use different policy language.

Having one industry standard policy, however, may not be a superior approach. Although determining important policy terms and conditions can be challenging to some insureds, the "flexibility" allows insureds to determine what policy language best suits their needs.

Some rules will serve as a guide to insureds, and their insurance agents and brokers, as they sort through the field of options.

1 Rule One: CGL Is Not Cyber

Some policyholders' counsel will argue that there is some coverage for cyber events under "traditional" insurance policies, such as commercial general liability, fidelity and crime policies, and even possibly in kidnap, ransom and extortion policies. If it is not explicitly excluded, then it is included, they suggest.

Carriers, however, almost always disagree and say that it is certainly not the intent of these policies to pick up cyber exposure. Changes have been made—and are being made—to these forms to clarify the intent. An early example occurred in 2001, when reinsurers implemented virus exclusions on reinsurance contracts, forcing primary CGL insurers to resist attempts to find coverage for third-party damages arising from computer viruses as well.

Additionally, if coverage is found under traditional policies, it is far from comprehensive. For instance, intellectual property infringement is excluded under recent versions of the Insurance Services Office (ISO) CGL policy, except for limited coverage for copyright in "advertisements," which is strictly defined and narrowly construed. Under the ISO language, property damage is limited to tangible property and excludes electronic data and software.

There has been one recent court case affirming limited coverage under a CGL policy—*Eyeblaster, Inc. v. Federal Ins. Co.*, (8th Cir. July 23, 2010). The specifics of the underlying case, however, involved a situation resulting in injury to a consumer's computer hardware caused by a software download, allowing the court to find coverage for "physical injury to tangible property." (See related textbox, "What The Court Said In Eyeblaster.") Keep in mind the key words "tangible property."

The variation in the approaches insurers are taking to cyber creates fantastic opportunities for brokers to bring value to insureds by being proactive and creative.

There are many other decisions that reach the opposite conclusion, including *America Online, Incorporated v. St. Paul Mercury Insurance Company,* (4th Cir.2003), often cited by legal experts as the leading case in this regard. The *America Online* court, determining that data was not capable of being touched, held that there was no physical damage to tangible property, lawyers note.

Insureds must also consider the time element and cash flow. Can they afford to litigate their CGL carrier in the hopes of securing coverage while at the same time covering the expenses of responding to a data breach? Does an insurance broker want to go through a costly E&O claim to defended himself or herself because coverage was denied by an insured's CGL carrier?

Sony's loss in early 2011 and subsequent coverage dispute with Zurich American Insurance Company highlights this issue. On July 20, 2011, Zurich filed suit against Sony contending that cyber insurance was not in place and that their traditional CGL policy only covered tangible losses.

2 Rule Two: Do not make assumptions based on policy labels, names of insuring clauses, endorsements, brochures, etc.

With no standard format or policy language for cyber insurance, a number of carriers have built exclusionary language, not in the "exclusions" section, but in the "definitions" section. For example, one carrier defines "wrongful act," in part, as "the theft or unintentional disclosure or mishandling of personal identifiable information that is in the care, custody or control of the Insured."

We like to see "unintentional disclosure" language, but the fact that the information must be in their control eliminates too many possibilities, the most obvious one being "clouding."

(CONTINUED ON NEXT PAGE)

What The Court Said in Eyeblaster

In *Eyeblaster, Inc. v. Federal Ins. Co.,* (8th Cir. July 23, 2010), the Eighth Circuit court, considering the "tangible property" issue, decided that an online marketing firm was entitled to defense-cost coverage.

In the underlying case, a consumer had alleged that the online marketer enticed him to visit an Internet that installed spyware, causing his computer to freeze and corrupting his operating system. The CGL policy defined property damage as "physical injury to tangible property, including resulting loss of use of that property."

"The plain meaning of tangible property includes computers, and the [consumer] complaint alleges repeatedly the 'loss of use' of his computer, the court ruled, affirming coverage for defense costs.

Of course, it's critical to check the exclusions section as well, which in one company's form, eliminates coverage for events "arising out of any actual or alleged failure to install available software product updates and releases, or to apply security-related software patches, to computers."

3 Rule Three: One size does not fit all

Know your Insured. Is your insured in the healthcare, e-commerce, professional services (legal, accounting, insurance) industries? Then privacy is high on the list of concerns.

Is it an international company? Then 'territorial" issues come into play, such as whether the "wrongful act" and claim be made anywhere? The Internet is worldwide.

Does the insured provide services to others for compensation? Then the technology E&O exposure must be addressed.

Brokers need to step back and understand the insured's business model prior to placing and negotiating policy language.

Brokers need to step back and understand the insured's business model prior to placing and negotiating policy language.

All too often, we see the wrong policy terms purchased, which do not address significant exposures of a particular insured. For example, we recently reviewed a policy for a children's clothing and accessories e-retailer. The e-retailer managed a blog that, among other things, gave medical advice to new parents. This was not a revenue-generating service, nor was it on the homepage of the website. The agent who represented the insured had missed a potential huge exposure—third-party damage arising from the "contextual liability." We feel that this exposure, at a minimum, has a contingent bodily injury exposure that needed to be brought to the insured's attention and addressed. We ended up carving out the bodily injury exclusion to NOT exclude contingent BI claims or allegations.

Some of the policies in the marketplace do not provide regulatory coverage, which would place the insured in a highly regulated industry in a significantly vulnerable position. State attorneys general and regulatory agencies, both on the state and federal level, are becoming increasingly more aggressive in protecting their constituents. For states facing large deficits and upcoming elections, imposing regulatory fines can increases state treasuries, while at the same time making great headlines.

4 Rule Four: One defense-coverage option does not fit all. Neither does one settlement-option

Got Defense? What will you choose: duty-to-defend or duty-to-pay?

Like most options, there are positives and negatives with each decision. Sometimes the choice is clear cut and the matter can easily be resolved based on the insured's size, ability to manage the litigation process and desire. In other cases, a modified approach incorporating something in between might be best.

For example, a duty-to-defend policy with pre-approved legal counsel might be best solution for an insured that is heavily involved in the technology industry. Maybe the company has retained qualified counsel, but prefers to have the administration of the litigation be managed by the insurance company. Other firms with large insured retentions and multi-layered insurance towers might feel more secure retaining counsel and managing the entire process.

Another consideration is policy language describing the insurer and insured obligations under a cyber insurance policy when both do not agree on whether to settle a claim. As with the defense provision, the selection of this language, often referred to as the "hammer clause," must be tailored to the insured's preferences. (See "Insureds Need To Support Out Potential Hammer Effects," for more information.)

5 Rule Five: Watch those sublimits

In determining which insurance company is offering the best options for an insured, it is important to consider the adequacy of sublimits applicable to individual coverage parts of cyber policies.

The most frequent sublimit discussed is for "notification expenses," closely followed by "rehabilitation." Rehabilitation refers to public relations expenses to minimize reputational damage of the insured. Depending on the insurance company, there may also be coverage available for costs of credit monitoring offered to breach victims. Notification and rehab expense can be covered under a single sublimit or separate ones.

Each carrier has its own unique names for its sublimited coverages, so be careful. One carrier's "breach-notification" coverage is another's "event-

management" expense, but both refer to the cost of notifying individuals whose personally identifiable information might have been compromised by a network security event. Dollar sublimits for this coverage can range from $150,000 to $1 million, although some carriers use a headcount approach (limiting the number of notifications that will be covered instead of imposing a monetary cap.) For large corporate accounts, we have arranged for excess carriers to drop down and follow underlying sublimits.

Notification expense can be significant, and the variables determining their magnitude include: the number of unique current records, the magnitude of historical records, and the geographical distribution of end users or customers. (See related textbox, "Compliance By State.")

The Ponemon Institute's *2010 Annual Study: U.S. Cost of a Data Breach*, estimated the average cost per compromised record at $214, up 5 percent from 2009. Clearly, at $214 per record, the cost of a data breach is more than all but the largest organizations can bear.

6 Rule Six: Covering the network may not be enough

In the 2010 survey, the Ponemon Institute noted that 35 percent of the breaches studied involved lost or stolen laptops or other portable data-bearing devices, eclipsing the percentage of breaches attributable to malicious or

(CONTINUED ON NEXT PAGE)

FOR MORE INFO

Compliance By State

Depending on the geographic reach of customers, there are potentially 47 different state laws (including the District of Columbia) with which an insured must comply.

- In 2001, California became the first state to have an agency dedicated to promoting the protection of consumer privacy rights when the Office of Privacy Protection opened. The Office was created by legislation in 2000.
- In 2002, California became the first state to pass privacy breach notification requirements with the passage of A.B. 700 and S.B. 1386, which became operative on July 1, 2003.
- Today, the only four states that do not have data loss/breach notification laws are Alabama, Kentucky, New Mexico and South Dakota.
- Of the 46 states that have notification legislation, 35 do not have a centralized reporting authority such as a Consumer Protection division or Attorney General.
- Many of the states' laws have unique clauses. For example, Massachusetts' law (Massachusetts General Law Chapter 93H/201 CMR 17.00) requires notification of any breach that involves one or more Massachusetts residents regardless of where the breach takes place or from where the entity who held the private information is domiciled or operating.
- Effective September 1, 2012, Texas will require notice to be provided to any individual who is either a resident of Texas, or a resident of a state that does not require notification of a security breach.

criminal attacks (31 percent) and those caused by system failures (27 percent). It follows then that a policy covering only one's network is not broad enough to cover one of the most prolific causes of a data privacy breach—loss of a portable data-bearing device.

7 Rule Seven: The underwriting process isn't necessarily over once cyber coverage is bound

Insureds typically think that filling out the application for coverage and any related attachments completes the application process—an event that occurs once a year.

That is not necessarily true in the world of cyber insurance. For example, one carrier includes the following clause deep in its policy wording:

"You [the insured] agree to notify us as soon as possible but in no event later than 30 days after [a] change to your business or network, including without limitation, any [of] your answers in the application, the nature, volume, value...of information stored, processed…on your network… We reserve the right to re-underwrite this policy and re-price premiums based on these changes."

Peter R. Taffae is managing director of Executive Perils, a Los Angeles-based national wholesaler solely dedicated to the D&O, E&O, EPL, fiduciary and cyber insurance. He may be reached at petert@eperils.com.

8 Rule Eight: Be proactive

All this variation in the approaches insurers are taking to cyber creates fantastic opportunities for brokers to bring value to insureds by being proactive and creative. Most underwriters will entertain custom language via endorsements so that the policy language addresses specific exposures of the insured.

More than most coverages, cyber policies fall under the maxim "buyer beware." The sage advice that says "you get what you pay for" applies here as well. A number of carriers have multiple cyber policies targeting different price points and offering different degrees of protection. Value is the objective—solid coverage at a fair cost. ■

FOR MORE INFO

The following websites offer more information on state breach notification and privacy laws:

Beazley's Data Breach Map
http://www.beazley.com/databreachmap

Baker Hostetler
http://www.bakerlaw.com/files/Uploads/Documents/Data%20Breach%20documents/State_Data_Breach_Statute_Form.pdf

http://www.bakerlaw.com/files/Uploads/Documents/Data%20Breach%20documents/Data_Breach_Charts.pdf

http://www.dataprivacymonitor.com/data-breach-notification-laws/

National Conference of State Legislatures
http://www.ncsl.org/issues-research/telecom/security-breach-legislation-2011.aspx