Cyber Liability: New Wrinkles on Old Coverage Issues

October 2012 - Issue XXV, Volume 10

By Stacey L. McGraw and Michael Kenneth

By now, surely everyone has received a letter from a major financial institution, a health care provider or a university that you o identifying information has been put at risk. Whether caused by a hacker who seeks the information for an identity theft schem "data breach" events are a well-known risk for any company or institution that collects personal data about its customers or emp sought coverage following these events-with mixed success-under general liability, professional liability, and commercial crime offering "cyber liability" or "cyber risk" policies specifically designed to protect against data breaches and other electronic injurie With recent SEC guidance that companies ought to disclose how they protect themselves against these types of risks and pote continuing to increase. The article also discusses how, despite the distinctly new risks at issue, we can expect familiar coverag related claims, and allocation-to drive the disputes that may arise between insureds and insurers.

The most prominent problem against which a cyber liability policy aims to protect is the data breach, where a malicious hacker customer information at risk. A recent study of data breaches analyzing claim payouts concluded that the average loss is $2.4 even include the expenses of the organization that suffered the breach. [1] While a data breach can involve lost customer data and/or lost employee data, the risks for which cyber risk policies can provide coverage often include other types of cyber-relate an organization receiving a computer virus, or passing along the same to a customer or other third-party, which itself can cause systems. Unfortunately, overzealous or rogue employees also are a source of risk, and they can cause trouble by slandering a company's electronically-stored information, or infringing on copyrighted materials.

An organization facing a data breach, or any other type of cyber risk, is likely to incur multiple types of damages. In the event o regulations governing how a company must provide notice to its customers (hence, the letters we receive all too frequently info risk), as well as the possibility of penalties for failing to protect data. Almost inevitably, there will be lawsuits, with the substantia at risk- through a data breach or malware attack-the organization will need to take steps to replace or protect its data and often business. In other words, cyber risks can entail significant first and third-party losses.

For companies with potential cyber risks, it is not a safe bet to rely on traditional policies to provide coverage. Claims for cover policies often are unsuccessful due to an inability to demonstrate property damage, which requires injury to tangible property, a does not meet. In addition, such property damage must be the result of an occurrence not caused by intentional acts to be cov data breaches and other cyber risks involve hackers and other criminal actors engaged in intentional wrongdoing. Insureds als that usually requires publication; lost data is (thankfully for us as consumers) often not seen by anyone. Still, whether a genera risks depends on the individual policies and the nature of the particular harms, so coverage disputes remain common. For exa breach events-a security breach at stores owned by Michaels and hackers accessing the data of Sony PlayStation users-insure confirm that their general liability policies do not provide coverage. [2]

Insureds may run into similar problems seeking coverage under errors and omissions policies. A typical professional liability po usually in connection with work performed for a customer, but excludes coverage for intentional wrongful acts. If a company's p tech-related activity, there is a greater likelihood of coverage for a cyber risk under an E&O policy. For example, in *Eyeblaster,* insured, an online marketing campaign management company, was sued by an individual who alleged that the insured's online spyware program that severely impaired the function of his computer, resulting in data loss, numerous pop-up ads, a hijacked b Circuit found that the allegations triggered a duty to defend under an E&O policy because Eyeblaster's activity of causing softw

the computer, while intentional, was not an intentional wrongful act. *See also Tagged, Inc. v. Scottsdale Ins. Co.*, No. JFM-11-
2011) (a professional services exclusion in a D&O policy applied to allegations that a social networking site's management false
children on their site because the allegations involved the professional service of regulating the content of the website). Howev
Co. of Pittsburgh, PA, 543 F.3d 7 (1st Cir. 2008), the insurer had no duty to defend allegations that an employee of the insured
reports as part of mortgage applications because intentional misconduct was excluded from coverage. Thus, for issues related
interactions with others, a standard E&O policy might provide some coverage, at least in responding to third-party claims. By c
the costs incurred by the victim company are either first-party losses or involve activity undertaken prior to a "claim" being made
otherwise complying with government regulations. Therefore, while an insured may be able to obtain reimbursement of litigatio
within the coverage of a typical professional liability policy.

For intentional wrongful acts not covered by CGL and professional liability policies, insureds can sometimes turn to commercial
area also include limitations that may be problematic in the typical cyber risk event. Specifically, commercial crime policies can
well as the loss of "future" income, which likely would limit an insured's ability to recover its own losses. Also, such policies ofte
information, which drives much of the costs and litigation arising from cyber risk. However, the Sixth Circuit recently ruled that
Secrets, Confidential Processing Methods, or other confidential information of any kind" did not exclude loss resulting from a co
a specific computer fraud rider to a crime policy. *Retail Ventures, Inc. v. National Union Fire Ins. Co. of Pittsburgh, Pa.*, Nos. 1
reasoned that, in context, the confidential information referred to in the exclusion was the insured's proprietary information, rath
rider provided coverage.

In light of the uncertainty of whether the typical menu of available coverage will cover losses from cyber risks, demand for insur
continues to grow. This demand has increased with the SEC Division of Corporate Finance's Disclosure Guidance on Cyberse
Disclosure Guidance recommended that companies should disclose the risk of cyber incidents for their particular business, as
risks, including a description of the relevant insurance coverage. While not creating an official requirement to purchase cyber li
this as a concern, more companies are becoming aware of the issue, including the litigation risks if they are not properly insure
question of whether the failure to purchase cyber liability insurance can open a company up to D&O claims for breach of fiducia
protecting the company against such risks if a cyber liability event occurs, or for not disclosing to shareholders knowledge of ina

While specific cyber liability policies-or endorsements to GL, E&O, or commercial crime policies addressing these risks-have be
relative infancy, without the standardization that is typical of policy forms in some more well-established areas. Third-party cyb
liability for permitting access to identifying information of customers (including information stored by third parties on an insured's
third party customer or business partner, or failing to notify a third party of their rights under the relevant regulations in the even
"advertising injury"-like harms through the use of electronic media, such as unauthorized use or infringement of copyrighted ma
First-party cyber liability coverage can include paying for the costs of providing notice to individuals whose identifying informatic
breach and taking steps to stop the breach; obtaining public relations services to counteract the negative publicity that can be a
losses; reimbursing the costs of responding to government investigations; and reimbursing the costs of replacing damaged hard
some companies offer reimbursement for damages to the insured entity caused by computer fraud; reimbursement for paymen
costs of responding to parties vandalizing the company's electronic data; and business interruption costs.

Although the new forms of cyber liability coverage address protecting data and using electronic media to communicate-risks as
traditional coverage issues well-known to coverage attorneys are still likely to be at the center of disputes between insureds and
consider its obligations to provide notice of circumstances, as well as notice of claims, in these new circumstances. What aspe
application? Does a known weakness in cyber security constitute circumstances that could lead to a claim? With whom does a
whether circumstances that could lead to a claim exist? In-house, will the Chief Technology Officer need to learn what constitu
Are there any vendors or other third parties who are responsible for a company's data that must be asked about potential claim
must it be reported to the carrier? Since occurrences such as a data breach are often public relations crises, what happens to
company takes action before involving its insurer? Companies will have to grapple with these issues, particularly when comple
possible flaws in security measures, while carriers similarly will have to consider how much information they will require about a
risk of providing coverage.

Of course, addressing new types of coverage-particularly ones that are not standardized-almost certainly will lead to coverage
example, a New Jersey federal district court recently ruled, on a motion to dismiss, that a liability policy may provide coverage f

internet calling company), causing the insured to lose the ability to process calls, its source of profit. *Vonage Holdings Corp. v.* Dist. LEXIS 44401 (D.N.J. Mar. 29, 2012). The relevant coverage language stated that the insurer

"will pay for loss of and loss from damages to 'money', 'securities' and 'other property' following and directly related to the use o property from inside the 'premises'…"

The carrier argued that a "transfer of that property" required the property to be physically taken, but the court rejected the argur policy language could be temporary, so the insurer's motion to dismiss was denied.

Policyholders and carriers also may debate whether multiple cyber liability claims are related, which can affect whether a claim *Westlabs, Inc. v. Greenwich Ins. Co.*, the Delaware Superior Court ruled that the claims against the insured-which involved both lawsuit potentially triggering coverage under a private company reimbursement policy-were related to claims preceding the poli matters were fundamentally identical. The court rejected the insured's argument that the earlier claim was resolved, and thus b acts were not interrelated because they involved different actions (e.g., the insured itself doing the "hacking," versus a third par No. 09C-12-048, 2011 Del. Super. LEXIS 261 (Del. Sup. Ct. June 13, 2011). Thus, the related claims language of both the pc company reimbursement policy applied to preclude coverage.

Coverage disputes may also arise from how cyber liability policies interact with other types of insurance policies when both pote intra-insurer disputes over allocation may have a new variable. For example, in the *United Westlabs* case, if, instead, both the traditional liability policy provided coverage, how would the carriers divide up the defense and the indemnity obligations? How *Westlabs*, if the litigation against the insured concerned the cyber extortion threat, would the cyber liability carrier be responsibl

We could identify potential coverage issues all day, but the problems that may arise are ones that would look familiar to any co thinking about how these "old" issues will intersect with 21 st century technology and a still-developing set of policies designed t

---

[1] Mark Greisiger, *Cyber Liability & Data Breach Insurance Claims: A Study of Actual Payouts for Covered Data Breaches* (Ne

[2] *Arch Ins. Co v. Michaels Stores, Inc.*, 1:12-cv-00786 (N.D. Ill., filed Feb. 23, 2012); *Zurich Am. Ins. v. Sony Corp. of Am.*, No

[3] SEC Division of Corporate Finance, *CF Disclosure Guidance: Topic No. 2, Cybersecurity* (October 13, 2011), http://www.se topic2.htm .

[4] Susanne Sclafane, *"'Just Get Me Coverage' Requests Come In To Cyber Brokers"* (Advisen, June 3, 2012).