LOS ANGELES & SAN FRANCISCO
Daily Journal
www.dailyjournal.com
WEDNESDAY, MAY 23, 2018

PERSPECTIVE

Courts wrestle with coverage of cyber-related claims

By Peter S. Selvin

Cyberinsurance is designed to fill an enterprise's coverage gaps, where coverage under other forms of insurance may not be triggered by these kind of losses. At the same time, and because cyberinsurance is a relatively new product, there are few reported cases involving coverage disputes. Importantly, those cases highlight the need for policyholders to scrutinize the menu of available coverage grants in any proposed cyberinsurance policy.

While to date there has been relatively few reported cases involving cyberinsurance coverage disputes, there has been much litigation surrounding whether traditional insurance policies will respond to cyber-related claims. Although there are some outlier cases finding coverage under a commercial general liability policy for some forms of cyber-risk (*Eyeblaster, Inc. v. Federal Insurance Company*, 613 F.3d 797 (8th Cir. 2010)), the majority view is that CGL policies ordinarily do not provide coverage for cyber-related risks. As the court held in *American Online v. St. Paul Mercury Insurance Company*, 347 F. 3d 89 (4th Cir. 2003), a CGL policy "does not cover the loss of instructions to configure the switches or the loss of data stored magnetically. These instructions, data and information are abstract and intangible, and damage to them is not physical damage to tangible property".

In this regard, consider the following scenarios:

• Where the data on an insured's computer have been stolen, or where it has been held hostage in connection with a ransomware attack, policyholders have sought to secure coverage under CGL and other traditional insurance products by arguing that its data was in fact "tangible property" within the meaning of a CGL policies. Although policyholders won some early victories on this point (*American Guarantee & Liability Ins. Co. v. Ingram Micro, Inc.*, WL 726789 (D. Ariz. April, 2000)), most courts do not consider the data residing on an insured's network to constitute "tangible property" within the meaning of a CGL policy. American Online; *Capitol Commission v. Capitol Ministries*, 2013 WL 5493013, *4 (E.D.N.C. 2013) (electronic data and computer software is intangible property).

While to date there has been relatively few reported cases involving cyberinsurance coverage disputes, there has been much litigation surrounding whether traditional insurance policies will respond to cyberrelated claims.

• When a hacker infiltrates an insured's computer, steals the insured's information and then posts the stolen data on the internet, policyholders have argued that this scenario meets the requirement of a "publication" as that word is typically used in Section B of the coverage grant of a CGL policy. The key question is whether there has been a "publication" where a third party, as distinct from the policyholder, "published" the material on the internet. This scenario played recently out in *Zurich American Ins. Co. v. Sony Corp*, 2014 WL 8382554 (N. Y. Sup. Ct. 2014). In that case a hacker infiltrated Sony's network and then posted the stolen information on the internet. While Sony argued that the third party's posting met the "publication" requirement under the company's CGL policy's, the court held that because Sony did not itself "publish" the pertinent information, there was no "publication" and hence no coverage under the policy. *But see Travelers Indemnity Co. v. Portal Healthcare Solutions*, 644 Fed. Appx. 245, 247-48 (4th Cir. 2016) (holding that the presence of information online itself constitutes a publication).

Policyholders have also faced challenges in seeking to secure coverage for cyber risks under crime policies. Thus, where an insured wires funds in reliance on an email that a fraudster has made to appear genuine, the insured has been "spoofed." In that instance as well, the majority view is that a crime policy will not afford coverage. *See, e.g., American Tooling Center v. Travelers Casualty and Surety*, 2017 WL 3263356 (6th Cir. 2017); *Apache Corporation v. Great American Insurance Company*, 2015 WL 7709584 (5th Cir. 2015); *Taylor & Lieberman v. Federal Insurance Company*, 2015 WL 3824130 (C.D. Cal. 2017). Although *Medidata*, 268 F.Supp.3d 471 (S.D.N.Y. 2017) went the other way, that case is now on appeal.

Aqua Star (USA) Corp. v. Travelers Casualty and Surety Company of America, 719 Fed. Appx. 701 (9th Cir. 2018), highlights the need for policyholders to scrutinize the available coverage grants offered by a particular policy. In that case, the policyholder sought coverage under a "computer fraud" policy for a loss of funds. That case arose from an incident in which its employees, in reliance on genuine appearing, but fraudulent, instructions, changed wire transfer information and thereby caused four wires to be sent to the fraudster.

Although not expressly discussed in the court's decision, it would appear that the policyholder in that case elected not to purchase socalled "social engineering" coverage. That form of coverage, which is often offered as an available option, would have protected the policyholder from the loss occasioned by the "spoofing" incident.

The other reported cases addressing coverage under a cyberinsurance policy, reinforce that the exclusions normally found in traditional insurance products may also limit coverage under in cyber in cyberinsurance policies.

Thus, in *P.F. Chang's v. Federal Insurance Company*, 2016 WL 3055111 (D. Arizona 2016), Chang's had entered into an agreement with a division of Bank of America. The agreement facilitated the pro-

cessing of credit card payments by Chang's customers. The agreement also obligated Chang's to reimburse the bank for any fees, fines, penalties or assessments incurred by the bank in taking remedial credit and identity theft steps arising from the data breach.

After Chang's experienced a data breach, the hackers exposed its customers' credit card information on the internet. As a result, the bank issued a $1.9 million assessment against Chang's, representing to the costs that the bank would have to incur to Chang's customers for reimbursements and credit and identify theft remediation.

Chang's tendered the claim under its cyber policy, but its carrier (Federal) denied the claim.

The court upheld Federal's denial of the claim on the ground that the policy, like many traditional insurance policies, excluded reimbursement for obligations, which Chang's had assumed under its contract with the bank. In other words, the customary exclusion for liability assumed under a contract came into play and foreclosed coverage.

Another general principle of insurance law foreclosed coverage under a cyberinsurance policy in *Travelers Property Casualty Co. v. Federal Recovery Services*, 103 F. Supp. 3d 1297 (D. Utah 2015). In that case, the insured had entered into a contract with a fitness company whereby it was to handle the electronic dues payments for the fitness company.

After the fitness company transferred its business to a former competitor, it requested that the insured transfer its electronic payment information to its successor. The insured refused, claiming that it was owed additional compensation for its services. When the fitness company sued the insured, it tendered its defense to Travelers.

The court determined that no defense was owed under the cyber policy. This was because the cyber policy only obligated Travelers to defend if its insured was sued for damages arising from any "error, omission or negligent act." Focusing on the fitness company's allegations that the insured had withheld the return of the electronic payment information knowingly and intentionally — essentially holding it hostage to the payment of additional compensation — the court held that the alleged acts did not fit within the coverage grant. *See also Resource Bankshares Corp. v. St. Paul Mercury Ins. Co.*, 407 F.3d 631, 635 (4th Cir. 2005).

***Peter S. Selvin** is a Partner at Ervin Cohen & Jessup LLP and head of the Firm's Insurance Coverage and Recovery Department. You can reach him at pselvin@ecjlaw.com*