haynesboone
Setting precedent.

Haynes and Boone's Newsroom

Insurance Coverage for Cyber Attacks
02/25/2013
Micah E. Skidmore

On Tuesday, February 19, 2013, information security firm Mandiant issued a report documenting computer security breaches at hundreds of organizations, allegedly resulting from a cyber-espionage campaign undertaken by elements of the Chinese government. The Mandiant report is only the latest i a series of much-publicized incidents of "hacking" performed by what is believed to be a variety of public and private actors. According to the Mandiant report and recent media accounts, the victims of these cyber attacks include a large number of American companies from the technology, financial, media, transportation, energy, construction, manufacturing, communications and legal industries.

The consequences of individual cyber strikes vary. In many cases, vast amounts of information, including trade secrets and private customer data, have been misappropriated for competitive advantage or other illicit purposes. Other incidents may result in damage to computer systems, including the destruction of proprietary data and loss of functionality in critical computer systems. Still other attacks may cause direct damage to other tangible property controlled by the computer systems that are compromised by hackers.

In response to the emerging threat of cyber assault, many insurers have begun marketing "cyber-liability" insurance policies. Depending on the policy form, these products may insure the policyholder against claims, including in some cases regulatory claims, arising out of a cyber event, such as denial o customer access, lost personal data, and some content related claims. While dubbed "liability" insurance, these products may also provide first-party coverage for (1) business interruption and data loss; (2) disclosure notification expense; and/or (3) crisis management and related public relations expense, in the event of a covered cyber event. Corporate policyholders should carefully consider the merits of cyber liability insurance in light of the increasing risk posed by public and private cyber actors.

For those corporate policyholders that have not yet purchased dedicated cyber liability policies, in the event of a cyber event, some traditional forms of coverage may provide protection against what is an increasingly complex menace to companies of all sizes. Commercial property insurance generally provides coverage for all risks of direct physical loss or damage to real and personal property, subject to exclusions. The loss of use of computer hardware and even data caused by a cyber attack may qualify as direct physical loss,[1] and the resulting damage, including business interruption, may be covered by a traditional commercial property policy, subject to the particular terms and exclusions that may be found in any given policy form. Likewise, the loss of an insured's product, the theft of trade secrets or other personal property in a cyber attack may also constitute physical loss or damage triggering coverage under a commercial property policy. Moreover, to the extent that there is no accompanying loss or damage to "data," the loss of valuable intellectual property or products may avoid exclusions relating to "software" or "data" related losses in some commercial property policy forms. Physical damage to property, such as the damage reported to a water pump from a cyber penetration at an Illinois utility in 2011,[2] would also fit within the coverage traditionally afforded by a commercial property policy.

Alternatively, traditional crime/fidelity policies may include coverage for loss of property caused by a third party resulting from the entry or deletion of data from a computer system. Depending upon the terms and exclusions found in a particular policy form, an insured may be entitled to coverage for the

loss of data or related property resulting from a cyber attack against the insured.

In spite of the ever increasing sophistication of cyber criminals, corporate policyholders should not overlook potential opportunities to recover losses from the basic coverage afforded by conventional commercial property and crime/fidelity policies.

If you would like assistance or more information regarding coverage for cyber attacks or any other insurance related matter, please contact one of the Haynes and Boone Insurance Coverage Practice Group partners listed below.

Erika L. Bright
214.651.5120
erika.bright@haynesboone.com

Werner A. Powers
214.651.5581
werner.powers@haynesboone.com

Matt W. Holley
214.651.5371
matt.holley@haynesboo

Micah E. Skidmore
214.651.5654
micah.skidmore@haynesboone.com

Ernest Martin, Jr.
214.651.5641
ernest.martin@haynesboone.com

David Taubenfeld
214.651.5531
david.taubenfeld@haynes

Leslie A. Thorne
512.867.8445
leslie.thorne@haynesboone.com

---

[1] *See, e.g., Lambrecht & Assocs., Inc. v. State Farm Lloyds*, 119 S.W.3d 16 (Tex. App.—Tyler 2003, no pet.); *American Guarantee & Liab. Ins. Co. v. Ingram Micro, Inc.*, 2000 WL 726789 (D. Ariz. 2000).

[2] *See, e.g.,* Ellen Nakashima, *Foreign Hackers Targeted U.S. Water Plant In Apparent Malicious Cyber Attack, Expert Says*, THE WASHINGTON POST (Nov. 18, 2011) (describing damage done to a water pump at an Illinois water utility through controls exerted from an IP address in Russia).