Cyber Spyware Found on U.S. Electric Grid Demonstrates Increasing Potential Exposures for Insurance Industry

June 2009

There have been increasing reports of cybercrimes in the past few years, many of them originating from sources outside the United States. Frequently, the attacks are by hackers targeting personal information for use in unauthorized financial transactions and other identity theft. Recently, however, there have been reports of a new target by "cyberspies": the U.S. electrical grid itself. These attacks demonstrate not only national security vulnerabilities, but also potential insurance exposures.

Recent reports that spies hacked into the U.S. electrical grid made instant headline news.[1] A grave vulnerability was exposed. Authorities investigating the intrusion reportedly found software tools left behind that could be used to destroy infrastructure components, and thus potentially disrupt service across the country.

Such exposure is not unique to our electrical grid. Potentially, other utilities including power and water companies with networked computer systems are vulnerable to cyber attacks. Hackers have taken advantage of this vulnerability in the past in other countries. In one reported case, a vandal infiltrated a computerized control system at a water-treatment plant in Australia, flooding parks and rivers with hundreds of thousands of gallons of sewage.[2] In another case, cyber-attacks caused a power outage, which was followed by a ransom demand from the hackers, in Central and South America.[3] The North American Electrical Reliability Corporation – the agency responsible for setting standards for the U.S. electrical grid – has stated that while it is working with the governments of the U.S. and Canada to improve the security of the electrical grid, "there is definitely more to be done." [4]

A disruption of the U.S. electrical grid or other utility system has the potential for causing a variety of substantial losses, many of which may be subject to insurance coverage or at least claims for coverage. The range of potential losses resulting from a power outage is illustrated by the "Northeast Blackout" of August 2003, when a massive widespread power outage occurred throughout the Northeastern and Midwestern United States, as well as the Canadian province of Ontario, affecting 55 million people. As might be expected, some of the resulting losses included disruption in industrial operations, retail sales, and other business interruption. Also attributed to the blackout was loss of water service due to the shutdown of electrical pumping systems; sewage spills into waterways; and the shutdown of the various railroad lines as well as regional airports. Spoilage of food due to the loss of refrigeration reportedly affected a large number of businesses and individuals.

Several recent decisions in coverage lawsuits arising from the Northeast Blackout demonstrate the potential exposure and coverage limitations for property as well as other lines of insurance. For example, one court held that an exclusion in a commercial property policy barring coverage for losses arising from off-premises failure of utilities precluded coverage for a grocery store's spoiled inventory as a result of the blackout.[5] However, in another case arising from the blackout, a federal court held that an exclusion pertaining to off-site power generation equipment in a boiler and machinery policy was ambiguous and therefore denied summary judgment to the insurer for a food company's claim for lost inventory.[6] Policies without such exclusions would potentially have significant exposures. Most recently, a New Jersey state court issued its ruling on a group of supermarkets' claim for food spoliation resulting from the blackout under a first party, all risk policy. [7] There, the court sided with the insureds and held that the interruption in electrical power was caused by "physical damage" to the electrical grid, thereby triggering the policy's "Services Away From Covered Location Coverage Extension" provision that extended coverage for consequential damages resulting from an interruption in electrical power caused by physical

damage to certain types of electrical equipment. The court reasoned that the power generation was "physically damaged" because it became incapable of performing its "essential function" – generating electricity – due to "a physical incident or series of incidents." These cases demonstrate the coverage uncertainty facing insurers and insureds alike in the aftermath of a utility failure.

In addition to the potential first-party insurance policy exposures resulting from a blackout, there is some potential for third-party insurance policy exposures if those sustaining blackout-related losses assert claims against the affected utility companies. A pair of cases relating to the Northeast Blackout demonstrates that utility companies may be targets of suits after a service failure, but also shows that maintaining such suits may be an uphill battle for the plaintiffs. In one, a class action suit filed within days of the Northeast Blackout, the trial court dismissed the suit for lack of subject matter jurisdiction, and the appellate court affirmed, on the basis that a state agency has exclusive jurisdiction over various matters concerning public utilities, including whether service rendered by a public utility is in any respect unjust, unreasonable, or in violation of law.[8] A New York court reached a similar result in dismissing a plaintiff's claim against Con Edison for food spoilage caused by the blackout, when it held that under the relevant state statute a utility company will not be held liable for an interruption of service resulting from causes outside of its control or due to mere negligence.[9] Although these cases suggest that maintaining such suits against utility companies can be difficult and an insurer's duty to indemnify under a third-party policy may not ultimately apply, an insurer that issues a third-party policy may still be required to defend a covered utility. In addition, the Schlesinger case suggests that a lawsuit may be tailored to bypass the limitation of liability provision of a statute, for example by including a reckless conduct claim. In such a case an insurer's duty to indemnify may ultimately come into play.

Finally, apart from traditional property, business interruption and liability policies, cyber risk policies may also be implicated in a blackout caused by hackers, although the wordings and scope of coverages vary greatly and thus applicability of such policies is uncertain. A number of insurers have recently introduced cyber risk policies.[10] Many cyber risk policies are tailored to cover data and privacy breaches resulting in potential or actual identity theft or impairment of web or server services to customers, or intellectual property infringement, rather than industrial or retail shutdown. However, broadly worded coverages for losses arising from alleged breach of a duty of care to limit transmission of malware that results in a denial of service potentially could be implicated, depending on the scope of coverage intended and the policy wording.

Due to the substantial risks and large losses involved, insurers and insureds alike would benefit from keeping an eye on this developing issue.

---

[1] *See, e.g., Siobhan Gorman, Electricity Grid in U.S. Penetrated By Spies*, WALL STREET JOURNAL, April 8, 2009; and Martin LaMonica, *Report: Spies Hacked Into U.S. Electrical Grid*, C-NET NEWS, April 8, 2009, available at http://news.cnet.com/8301-11128_3-10214898-54.html.

[2] *See Marshal Abrams and Joe Weiss, Malicious Control System Cyber Security Attack Case Study–Maroochy Water Services, Australia*, available at http://csrc.nist.gov/groups/SMA/fisma/ics/documents/Maroochy-Water-Services-Case-Study_report.pdf (last visited April 27, 2009).

[3] William Lowther, *CIA Launches Hunt for International Computer Hackers Threatening to Hold Cities Ransom by Shutting Down Power*, MAIL ONLINE, available at http://www.dailymail.co.uk/news/article-509186/CIA-launches-hunt-international-hackers-threatening-hold-cities-ransom-shutting-power.html (last visited April 27, 2009).

[4] *NERC Statement on Cyber Security & the Electric Grid*, April 8, 2009, available at: http://www.nerc.com/news_pr.php?npr=279 (last visited April 27, 2009).

[5] *Four Star Bros., Inc. v. Allied Ins. Co.*, Docket No. 04-CV-73401, 2006 WL 148754 (E.D. Mich. Jan. 19, 2006).

[6] *Tufo's Wholesale Dairy, Inc. v. CAN Financial Corp.*, Docket No. 03 Civ. 10175, 2005 WL 756884 (S.D.N.Y. April 4, 2005).

[7] *Wakefern Food Corp. v. Liberty Mutual Fire Ins. Co.*, Docket No. A-2010-07T3, 2009 WL 1065979 (N.J. Super. A.D., April 22, 2009).

[8] *Ippolito v. First Energy Corp.*, Docket o. 84267, 2004 WL 2495665 (Ohio App. 8 Dist., Nov. 4, 2004).

[9] *Schlesinger v. Con Edison Co. of New York, Inc.*, Index No. 6142/03, 2003 WL 22964883 (N.Y. City Civ. Ct., Dec. 16, 2003).

[10] Also known as E-Commerce Insurance, E-Business Insurance, Information Security Insurance, Cyber Insurance, Network Security Insurance or Hackers Insurance.