Portfolio Media. Inc. | 860 Broadway, 6th Floor | New York, NY 10003 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

Cyberattack Insurance Challenges Confront Energy Sector

Law360, New York (October 29, 2014, 10:46 AM ET) -- There have been numerous cyberattacks on retail, financial and e-commerce businesses in the last year, affecting millions of customers and hundreds of millions of dollars in response costs. Now it appears the threat of a cyberattack poses an even greater exposure risk to the energy sector — and there is no comprehensive insurance coverage to respond to such an attack.

Glenn R. Legge

Energy companies use vast amounts of data for exploration, equipment maintenance, critical infrastructure, remote environmental controls and safety systems, as well as for optimizing exploration and production costs. This represents an exponential increase in the data points vulnerable to cyberattack. Companies rely on supervisory control and data acquisition and other industrial control systems that manage worldwide exploration and production operations on land, offshore and in deepwater environments.

Pipeline operators use remote detection and control systems to measure pressure, temperature and corrosion in thousands of miles of pipelines on land and offshore. Deepwater drillships, services vessels and oil tankers use GPS and electronic chart display and information systems to aid navigation and vessel traffic control. The petrochemical industry uses SCADA and ICS systems to regulate processing of hydrocarbons and chemicals.

Cyberattack Exclusions are Common

The federal government has recognized the tangible threat of cyberattacks on the energy sector and has spent considerable time and expense creating programs to assist in preparing for this peril.

In May 2013, the U.S. Department of Commerce issued guidelines for SCADA systems, after recognizing various probable cyber risks, including unauthorized changes to instructions, commands or alarm thresholds, which could damage, disable or shut down equipment, create environmental impacts and endanger human life.

In February 2014, the U.S. Department of Homeland Security and U.S. Department of Energy issued the Oil and Natural Gas Subsector Cybersecurity Capability Maturity Model (ONG-C2M2). The C2M2 program was created to enable energy companies to effectively and consistently evaluate and benchmark their cybersecurity capabilities.

The federal government also realized that, although the energy sector has billions of dollars of insurance for risks ranging from pollution, property damage, business interruption and bodily injury, much of this insurance may not provide coverage for damages arising out of cyberattacks due to exclusions in these policies. In July 2014, the DHS reported that cyber-risk exclusions are “common place in property insurance written for the energy sector companies.”

Enhanced Corporate Responsibility to Manage Risk of Cyberattacks

On June 10, 2014, Securities and Exchange Commissioner Luis Aguilar recognized the growing frequency and severity of cyberattacks and advised the New York Stock Exchange that "ensuring the adequacy of a company's cybersecurity measures needs to be a critical part of a board of director's risk oversight responsibilities." Aguilar highlighted various best practices for companies guarding against a devastating cyberattack, including the review and assessment of corporate insurance policies.

Are Energy Cyberattacks a Realistic Threat?

On July 12, 2014, The Economist reported that although SCADA systems may be removed or protected from direct connections with the Internet, they are not necessarily secure from evolving cyberattacks. In fact, credible cyber-risk threats to the energy sector appear to have increased in 2014 based on various sources:

- On June 20, 2014, the Houston Chronicle FuelFix blog reported that "a network of hackers called AnonGhost says it has launched a barrage of cyberattacks on international energy companies" in the Middle East and the U.S.

- On July 2, 2014, the DHS' Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) warned energy companies of malicious software used by "a Russian hacking group known as 'Energetic Bear' or 'Dragonfly' ... that primarily targets the energy sector and related industries."

- On Oct. 16, 2014, DHS ICS-CERT advised of vulnerabilities in a Siemens OpenSSL that would allow a "man-in-the-middle" attack to hijack a session between an authorized user and the device. The affected Siemens products are used for process and network control and monitoring in critical infrastructure such as chemical, critical manufacturing, energy and wastewater systems.

Can Companies Find Insurance to Cover Cyberattacks?

Now that the U.S. Securities and Exchange Commission has encouraged corporations to maintain adequate insurance, the challenge may be in finding and obtaining such insurance coverage. Perhaps the first question to be asked by corporate risk management is "what type of damages would arise from a cyberattack?"

Damages from energy-related cyberattacks can include pollution and property damage to business interruption and loss of confidential/financial information. These claims would not be covered under a singular policy of insurance. Therefore, coverages must be assembled from a variety of policies.

The energy sector, on the whole, is well-insured, either through commercial insurance policies, self-insurance, captive insurance or a combination of all three types. In addition, the vast majority of property, liability or environmental insurance policies are reinsured to some degree.

Although the upstream, midstream and downstream energy markets are well-insured, many of these insurance policies contain exclusions for damages arising out of cyberattacks, malevolent viruses or malware. The end result is an ocean of insurance coverage, but barely a drop that would cover catastrophic damages arising from a cyberattack.

Cyber-Risk Policies with Low Limits

Currently, there are some cyber-risk insurance policies that provide limited coverage for first-party

and third-party claims with relatively low limits, ranging from between $10 million to $25 million. Although claims related to property damage and business interruption generally have not been covered under cyber policies, in the last year, the insurance industry has offered new policies that provide some coverage for these types of damages. The majority of these provide coverage for data breaches and the disclosure of personally identifiable information derived from credit cards, drivers' licenses and Social Security numbers. They do not appear to provide coverage for catastrophic environmental, bodily injury or property damage/business interruption damage models that could result from a cyberattack on an energy company. In the last six months, more innovative and broader coverages have been developed by various underwriters in the London insurance market.

Directors and Officers Insurance

D&O policies may provide some coverage to corporate management and the entity for securities claims related to alleged failures to mitigate cyber risks. D&O policies will not provide coverage for damages to property of the corporation or third parties.

Property Insurance

Property insurance insures the corporation's physical assets, however such policies often exclude cyber risks. In addition, there is some question as to whether damage to software and computer systems equate to property damage, which is frequently defined as "physical damage to tangible property." Also, many property policies contain exclusions for damages arising from cyberattacks.

Upstream Energy Insurance Facilities

Oil Insurance Limited is a Bermuda-based mutual insurance program for the energy industry. The coverage provided by OIL includes property damage, control-of-well, redrill, and pollution coverage. Although OIL does not provide coverage for claims related to war risks, it does provide some degree of coverage for cyberattacks on its members. The aggregate limit of OIL coverage is $750 million per event.

Chrysalis is a specialized excess insurance program underwritten by London market insurers that provides coverage for exploration and production companies. The policy terms provided by Chrysalis are similar to those provided by OIL in that they provide some amount of coverage for cyber risks. Chrysalis also provides up to $125 million per occurrence for cyberattacks.

Commercial General Liability Insurance

CGL insurance coverage is the most common form of liability insurance that covers claims of third parties related to property damage and bodily injury (Coverage A), as well as personal and advertising injury (Coverage B). Some courts have interpreted CGL policies to cover certain types of damages arising from cyberattacks. Endorsements added to CGL policies can also provide coverage for some pollution liability. Cyber-risk coverage under CGL policies is largely determined by the facts of the underlying cyber intrusion. U.S. courts are divided as to whether claims for property damage and publication of confidential information are covered under CGL policies.

In 2004, Insurance Services Offices Inc., an insurance industry association that develops standardized insurance terms, revised the definition of property damage to exclude electronic data. That same year, ISO redefined its electronic data exclusion to preclude coverage "arising out of the loss of use of, damage to, corruption of, inability to access or inability to manipulate 'electronic data' that does not result from physical injury to tangible property."

In other words, if a company suffers catastrophic damages because of loss of use of electronic data due to a cyberattack, there is likely no coverage. On the other hand, if an energy company suffers catastrophic damage from loss of use of electronic data because a meteor or some object struck a computer/SCADA/ICS equipment and knocked it off line, then the company may have coverage.

New and Existing Policy Exclusions for Cyber Risks

Various insurers have introduced limited cyber-risk policy exclusions over the last decade, some of which have been litigated in U.S. courts. The London insurance market began to use the NMA 2914 exclusion in 2001 and the CL380 exclusion in 2003. These exclude coverage for loss, damage or alteration of electronic data or damage liability or expense arising from a computer, software program, malicious code or computer virus used as a means for inflicting harm. These exclusions are commonly used in primary, excess and reinsurance policies for energy, marine and nonmarine risks. They have not been tested in any reported court opinions in the U.S. or U.K., however it is not unreasonable to expect they will be tested in a coverage suit at some point.

On May 1, 2014, ISO activated new comprehensive data breach exclusions focused on preventing any coverage under widely used CGL policies. Many of these new exclusions appear to be focused on disclosure of confidential information and "data-related" liability.

Various insurance brokers have urged insurers and underwriters either to lessen the scope of these exclusions or eliminate them entirely in an effort to provide a more comprehensive insurance cover for the energy sector. Many of these brokers acknowledge, however, that the reinsurance market also uses many of these cyber-risk exclusions. Therefore, the direct insurers cannot reinsure any of the risks arising from a cyberattack.

How Do Energy Companies Secure Adequate Insurance for Cyber Risks?

Unfortunately, the majority of companies in the energy sector will be under pressure from regulators to forage for adequate cyber-risk coverage among a variety of policies on the market. To date, domestic and international underwriters have not offered comprehensive catastrophic coverage for losses or liabilities arising out of cyberattacks on energy companies. The current policy exclusions may be motivated by the extensive first-party and third-party claims that could arise from a cyberattack on an upstream, midstream or downstream company. It would be challenging to set a fair premium to cover such a substantial pool of risks, and it's likely many companies would find the necessarily high cost of cyber-risk insurance to adversely impact their financial bottom line.

The existing and new data breach and cyberattack exclusions will be tested in the courts with a patchwork of opinions providing little predictability to companies working domestically and abroad. Due to the variety and amount of losses that could arise from an attack on the infrastructure of an energy company, it is unlikely that a comprehensive liability, property and cyber-risk coverage will be developed to fit the needs of industry. The good news is that the insurance industry, particularly the London insurance market, is very familiar with the energy sector and will continue to respond to its need for evolving coverage of cyber risks.

—By Glenn R. Legge, Jeanie T. Goodwin and Jacob C. Esparza, Legge Farrow Kimmitt McGrath & Brown LLP

Glenn Legge is a partner and Jeanie Goodwin and Jacob Esparza are associates in Legge Farrow Kimmitt McGrath & Brown's Houston office.