CYBER-PHYSICAL ATTACKS ON CRITICAL INFRASTRUCTURE: WHAT'S KEEPING YOUR INSURER AWAKE AT NIGHT?

Date: 24 January 2017

By: James E. Scheuermann

Cyber-physical attacks on critical infrastructure that have the potential to damage those physical assets and to cause widespread losses to third parties are keeping your insurer awake at night. A cyber-physical attack on critical infrastructure occurs when a hacker gains access to a computer system that operates equipment in a manufacturing plant, oil pipeline, a refinery, an electric generating plant, or the like and is able to control the operations of that equipment to damage those assets or other property. A major cyber-physical attack on critical infrastructure is a risk not only for the owners and operators of those assets, but also for their suppliers, customers, businesses and persons in the vicinity of the attacked asset, and any person or entity that may be adversely affected by it (*e.g.*, hospital patients and shareholders).

Because damages caused by a cyber-physical attack can be widespread, massive, and highly correlated, affecting multiple sectors of the economy and many lines of insurance, the insurance industry is giving this risk heightened attention. The U.K. insurance marketplace Lloyd's, London and the University of Cambridge, for example, conducted a major study of the losses resulting from a hypothetical cyber-physical attack on 50 electrical generators in the Northeast U.S. Other insurance market participants have also published reports addressing cyber-physical risks to critical infrastructure.[1] The insurance industry's focus on cyber-physical risks perhaps should be action-guiding for corporate policyholders as well.

To date, there have been only two major publicized cyber-physical attacks. The first was the use, in 2008 through 2010, of the Stuxnet virus to destroy approximately 20% of Iran's centrifuges used to make nuclear materials. Stuxnet reportedly damaged the centrifuges by causing them to spin out of control.[2] In the second attack, in late 2014, the hackers gained access to the computers of a German steel mill through a minor support system for environmental control. The attack led to the destruction of a blast furnace in the steel mill. German authorities did not allow the publication of many details of the attack, but they did describe the resulting damage as "massive."[3]

Several attacks on critical infrastructure did not result in property damage beyond the infected computers themselves, but apparently only because of fortuitous events or the narrow goals of the attackers. Some well-publicized examples of such attacks include:

- An attack on the Ukraine power grid in December 2015. This was a multistage, multisite attack that disconnected seven 110 kV and three 35 kV substations and resulted in a power outage for 80,000 people for three hours. The attackers' point of entry – a phishing scam.[4]
- In 2014 the "Energetic Bear" virus was discovered in over 1,000 energy firms in 84 countries. This virus was used for industrial espionage and, because it infected industrial control systems in the affected

facilities, it could have been used to damage those facilities, including wind turbines, strategic gas pipeline pressurization and transfer stations, LNG port facilities, and electric generation power plants. It has been suggested that a nation-state "pre-positioned attack tools to disrupt national scale gas suppliers."[5]

- A small flood control dam 20 miles north of New York City was hacked in 2013. The attacker would have been able to control the sluices but for their being taken off-line for maintenance.[6] One report suggested that the attackers intended to hack a dam of the same name in Oregon many times the size of the New York dam.[7]
- Last November hackers destroyed thousands of computers at six Saudi Arabian organizations, including those in the energy, manufacturing, and aviation industries. The attack was aimed at stealing data and planting viruses; it also wiped the computers so they were unable to reboot. This attack was similar to a 2012 attack on Saudi Aramco, the world's largest oil company, which destroyed 35,000 computers. [8]

These are not isolated incidents.[9]

The scope of the cyber risk to critical infrastructure is multiplied when cyber is viewed not as a discrete risk, but as "being an enabling and amplifying factor for existing categories of risk."[10] If the non-cyber risk of fire or explosion at an oil refinery is X, then including in the risk calculation the probability of that fire or explosion being caused by a cyber attack leads to a risk of multiples of X.

Insurers in cyber insurance markets are struggling to find the appropriate multiple of X for cyber-physical risks in circumstances of too little reliable cyber-risk relevant information. For U.S.-based risks, the difficulty stems in part from too little publicly available, reliable information on the number, types, severity, and scope of cyber attacks on critical infrastructure. Corporate victims generally do not publicly disclose cyber-physical attacks. Similarly, the U.S. Department of Homeland Security does not publicly disclose successful cyber attacks on critical U.S. infrastructure. That leaves insurers assessing risk from other sources whose information may be inaccurate or incomplete.[11]

In addition to too little information, market participants point to three attributes of cyber-physical risk that present difficult challenges for the pricing and underwriting of cyber policies. First, cyber risks present systemic exposure – a cyber-physical attack can cause widespread and highly correlated harm across broad geographical areas and multiple sectors of the economy.[12] The Lloyd's study estimated that a cyber-physical attack on 50 generators in the U.S. Northeast could cut power to 93 million people and result in $243 billion to $1 trillion in economic losses, and $21 billion to $71 billion in insurance claims.[13] For comparison, Super Storm Sandy in 2012 resulted in approximately $100 billion in damages[14] and the U.S. GDP in 2015 was just under $18 trillion.

Second, cyber attacks are "intangible" in the sense that the perpetrators often remain anonymous and an attack can go undetected for many months.[15] Malware and viruses may be installed now in the computers controlling a piece of infrastructure and still be undetected. Assessing the random probability of loss, the traditional core task of underwriters, in the face of "unknown unknowns" is a challenge.

Finally, the risk is dynamic. The types of attacks, their targets, and the nature of the attackers (nation-states, terrorists, hacktivists, criminals, the teenager next door) and their motivations (espionage/sabotage, political goals, financial gain, curiosity/malice) are constantly evolving.[16] There are virtually unlimited avenues by which such attacks can be mounted, including phishing scams, "watering hole" scams,[17] the infection of industrial

control systems software as it is being developed (one of the methods employed by the Energetic Bear hackers), an attack on Internet Exchange Points that form the interfaces between different computer networks,[18] the millions of unsecured and unencrypted devices that are part of the Internet of Things,[19] and the actions of rogue employees.

These underwriting challenges are also risk-assessment and risk-management challenges for corporate boards of directors and risk managers. This is especially so when these challenges have had a direct impact on cyber insurance markets. The general consensus in the insurance industry is that cyber-physical risk is underinsured. Note, for example, in the Lloyd's study mentioned above that the estimated insurance claims from the hypothetical attack on the electric power generators are less than 10% of the estimated damages. This underinsurance of cyber-physical risk is reflected in part in prevalent exclusions for bodily injury and property damage resulting from a cyber incident found in most first-party and third-party cyber insurance policies.

For corporate policyholders that own or operate critical infrastructure, managing cyber-physical risks in this insurance environment may require greater creativity than normal. The use of a captive insurer, for example, may be an attractive way to self-insure the first layer of cyber-physical risk. Some insurers are selling primary layer wrap policies that are intended to cover property damage losses excluded under most primary layer cyber policies. Difference-in-conditions excess policies that drop down to provide property damage coverage excluded in the underlying policy are also being marketed by certain insurers. Finally, because cyber insurance typically is negotiable, policyholders may attempt to negotiate terms that eliminate altogether or minimize the scope of exclusions for property damage or bodily injury caused by a cyber attack. London-market Form NMA 2915, for example, provides coverage for physical damage to property directly caused by fire or explosion if the fire or explosion itself was caused by a cyber event such as the loss or destruction of electronic data or a computer virus.

For corporate policyholders that do not own or operate any critical infrastructure but whose operations are critically dependent upon it – virtually the rest of the corporate community – a major cyber-physical attack on critical infrastructure may have profound adverse financial impacts. Consider a cyber-physical attack in which the attacker uses its operational control of a piece of critical infrastructure to cause that facility to explode or catch fire. The resulting property damage, personal injuries, and economic losses could be enormous. The potential defendants in the resulting class actions could well include: the owner of the infrastructure, the operator, the directors and officers of the corporations (in shareholder derivative actions), the manufacturers of the digital devices through which the attack was made, developers of the control system software, developers of the security software providing firewalls and malware protection, and any other designer of those devices.[20] Third-party general liability coverage and other liability coverages (such as E&O and D&O coverages) with adequate limits may be essential to the financial health of any defendant.

Independent of the exposure represented by potential litigation, which implicates third-party liability coverage, a corporate policyholder upstream or downstream of critical infrastructure that has been attacked will want coverage for its first-party losses. Those losses may include property damage, economic losses from interruption of its business or the businesses of its vendors, environmental damages, the extra expenses incurred to minimize business interruption losses, and loss of data. Accordingly, a policyholder who does not own infrastructure but who may be affected by a cyber-physical attack on it will want to have in place adequate and unambiguous first-party coverage for property damage, business interruption, contingent business interruption, and extra expense.

New and heightened cyber-physical risks merit increased policyholder attentiveness to both traditional (not-cyber-specific) first-party property and third-party liability coverages previously believed to be relatively routine and to the terms of cyber insurance policies being considered or already purchased. This is especially the case when Lloyd's itself has noted that first-party property coverages "are commonly silent on whether cyber-related losses would be paid," and that this is likely to lead to coverage disputes.[21] Lloyd's has further noted "key areas of uncertainty and ambiguity" in the scope of coverage for cyber-physical losses.[22] The risk of a cyber-physical attack on critical infrastructure extends broadly across the economy. Corporate policyholders may find it prudent to review carefully their traditional first-party and third-party coverages and their cyber coverage in light of this evolving and dynamic risk.

Notes:

[1] Lloyd's "Business Blackout, The Insurance Implications of a Cyber Attack on the U.S. Power Grid" (2015), available at www.lloyds.com/~/media/files/news%20and%20insight/risk%20insight/2015/business%20blackout/business%20blackout20150708.pdf ("Lloyd's, Business Blackout"); *see also, e.g.*, Willis Towers Watson, "Energy Market Review" (April 2016), available at www.willis.com/naturalresources/pdf/EMR2016/WillisTowersWatsonEMR2016.pdf ("Willis, Energy Market"); World Energy Council (in partnership with Marsh & McLennan Companies and Swiss Re Corporate Solutions), "World Energy Perspectives, The road to resilience" (2016), available at http://www.worldenergy.org/wp-content/uploads/2016/09/20160926_Resilience_Cyber_Full_Report_WEB-1.pdf ("World Energy Council"); The Geneva Association, "Ten Key Questions on Cyber Risk and Cyber Insurance" (Nov. 2016), at pp. 26-28, available at www.genevaassociation.org ("Ten Key Questions"). *See also* the President's Commission on Enhancing National Cybersecurity, "Report on Securing and Growing the Digital Economy" (Dec. 1, 2016), available at https://obamawhitehouse.archives.gov/sites/default/files/docs/cybersecurity_report.pdf.

[2] "Stuxnet was work of U.S. and Israeli experts, officials say," *The Washington Post* (June 2, 2012), available at https://www.washingtonpost.com/world/national-security/stuxnet-was-work-of-us-and-israeli-experts-officials-say/2012/06/01/gJQAlnEy6U_story.html?utm_term=.6ce5ab99f4b1; Lloyd's, Business Blackout, at p. 46.

[3] Willis, Energy Market, at p. 21; "How to stop cyber-attacks on your organization," *The Guardian* (Oct. 14, 2015), available at www.theguardian.com/public-leaders-network/2015/oct/14/how-to-stop-cyber-attacks-on-your-organisation.

[4] World Energy Council, at p. 19.

[5] Willis, Energy Market, at p. 21; "Russian Hackers Targeting Oil & Gas Companies," *The New York Times* (June 30, 2014), available at www.nytimes.com/2014/07/01/technology/energy-sector-faces-attacks-from-hackers-in-russia.html?_r=0.

[6] "Iranian Cyber Attack on New York Dam Shows Future of War," *Time* (Mar. 24, 2016), accessed at www.time.com/4270728/iran-cyber-attack-dam-fbi/.

[7] World Energy Council, at p. 35.

[8] "Hackers destroy computers at Saudi aviation agency," *CNNMoney* (Dec. 2, 2016), available at http://money.cnn.com/2016/12/01/technology/saudi-arabia-hack-shamoon/; "Cyberattacks Strike Saudi Arabia,

Harming Aviation Agency," *The New York Times* (Dec. 1, 2016), available at http://www.nytimes.com/2016/12/01/world/middleeast/saudi-arabia-shamoon-attack.html?_r=0.

[9] *See* World Energy Council, at p. 6 (identifying additional cyber attacks on critical infrastructure worldwide). Consider also (1) that 80% of oil and gas companies experienced a rise in the number of successful cyber attacks from 2014 to 2015, World Energy Council, at p. 10, and (2) the Department of Homeland Security Industrial Control Systems Cybersecurity Emergency Response Team responded to 295 cyber incidents within the energy sector in 2015, a 20% increase over 2014 (*id*. at pp. 10-11).

[10] Willis, Energy Market, at p. 20.

[11] *Id*. at p. 22; Ten Key Questions, at pp. 10, 14, 17.

[12] Lloyd's, Business Blackout, at pp. 3, 25; Ten Key Questions, at p. 14.

[13] Lloyd's, Business Blackout, at p. 3.

[14] World Energy Council, at p. 21.

[15] Lloyd's, Business Blackout, at p. 3.

[16] Lloyd's, Business Blackout, at pp. 3, 25; Ten Key Questions, at pp. 14, 29.

[17] A "watering hole" attack infects a website that the hacker's victim often visits with malware; visiting the site downloads the malware to the victim's computer.

[18] Ten Key Questions, at p. 27. Critical infrastructure includes the global internet itself, including its regional components.

[19] *See* "Here's how the 'Internet of Things' is being used for major cyber attacks on corporations," *Business Insider* (Oct. 21, 2016), accessed at http://www.businessinsider.com/internet-of-things-corporate-cyberattacks-2016-10; *see generally*, U.S. Dept. of Homeland Security, "Strategic Principles for Securing the Internet of Things" (Nov. 15, 2016), available at www.dhs.gov/securingtheiot.

[20] *See* Lloyd's, Business Blackout, at pp. 29, 31.

[21] Lloyd's, Business Blackout, at p. 37.

[22] *Id*.

