Energy Sector Beware: Cybersecurity Now Top Security Threat

Action Item: A cyber-attack on American energy facilities and/or infrastructure could bring unparalleled catastrophe. Our enemies are already probing our perimeters. Particular vulnerabilities for the oil and gas sector exist at “single-point” assets such as refineries, storage terminals, and other buildings, as well as “networked features” such as pipelines and cyber systems. Business leaders and elected officials must rise to thwart the threat. The Pennsylvania Public Utilities Commission is showing great leadership with its recent “summit” and publication of its “Cybersecurity Best Practices for Small and Medium Pennsylvania Utilities” plan, which gives good leads on how to counter this live threat.

What is the number one worldwide security threat? The answer is cybersecurity. This is especially so for our critical energy production and delivery infrastructure.

This issue has even taken hold in mainstream entertainment. Earlier this year, Hollywood released the hacker movie Blackhat, which Wired.com called “the best hacker movie ever made.” The movie centers around a cyber-attack on a nuclear power plant in Hong Kong that results in the collapse of a cooling tower and places the plant on the verge of a meltdown. The movie was inspired by Stuxnet, a computer worm developed during the George W. Bush administration, which destroyed nearly one-fifth of Iran’s nuclear centrifuges.

But this is not Hollywood; it’s very real, very dangerous, and very eschatological. A cyber-attack presents the risk of unfathomable asymmetrical physical damage to life and property, as well as the potential for flat-lining the enterprise value of any targeted company. A Congressional Commission has estimated that in a prolonged nationwide blackout (this in the context of an Electromagnetic Pulse (“EMP”) attack), about 90 percent of the U.S. population would be dead from disease, lack of food and resources, and societal breakdown. That 90 percent won’t care whether the nation was struck by an EMP attack or a cyber-attack.

According to the U.S. Department of Homeland Security (“DHS”), over the past several years the energy sector has incurred the greatest number of cybersecurity incidents. Pennsylvania Public Utility Commissioner Pamela Witmer summed it up at the PUC’s recent, one of a kind, multi-agency summit on cybersecurity: “According to the U.S. Director of National Intelligence, cybersecurity is the number one security threat worldwide, ranking higher than terrorism, espionage, and weapons of mass destruction.”
Commissionsr Witmer made this statement at the October 1, 2015, press conference kicking-off the PUC’s cybersecurity summit, which was intentionally timed with National Cybersecurity Awareness Month. The PUC, to its credit, gathered in one room the DHS, as well as state and local agencies including the Office of Administration, the Pennsylvania Emergency Management Agency, the Pennsylvania State Police, and the Pennsylvania Office of Homeland Security, and several large utilities, including UGI Utilities, Pennsylvania American Water, Verizon Pennsylvania, and PPL Electric Utilities, to vet this problem and talk about preparedness, prevention, and solutions.

So far, so good in Pennsylvania in getting the job done to protect critical energy infrastructure from cyber-attacks. But, the summit stressed that the danger is not going away and that we must constantly work together to stay vigilant. Indeed we must. According to a Wall Street Journal report, a survey of 625 IT executives in the U.S., U.K., France, and Germany found that 48 percent said they think it is likely there will be a cyber-attack on critical infrastructure, including energy infrastructure, in the next three years that will result in the loss of life. The costs of cybersecurity are also increasing at an alarming rate. For example, JPMorgan Chase’s annual cybersecurity expenditures are expected to double to $500 million within the next five years.

What are the threats, you ask? They are too numerous to list in this article, but here are a few: the Havex Trojan targets industrial control systems after it is mistakenly downloaded by customers; Malware called BlackEnergy has targeted systems used in nuclear power plants; and an Iranian hacking campaign is underway that the FBI believes may be targeting the energy and defense industries. The Chinese, Russians, and North Koreans can be added to the list of “usual suspects” as cyber-crime, cyber-espionage, and cyber-sabotage have increasingly become their weapons of choice lately—and recent events show they are good and getting better at it. ISIS is also considered a dire threat in this regard.

In fact, nationalized cyber-weaponization has become the norm for our enemies. According to National Intelligence Director James Clapper, Russia’s Ministry of Defense is establishing its own cyber command, which is expected to conduct offensive cyber activities such as inserting malware into enemy command and control systems. In May 2014, the U.S. Department of Justice indicted five officers from China’s Peoples’ Liberation Army on charges of hacking U.S. companies. U.S. officials have also linked an Office of Personnel breach to China, which compromised the personal information of more than 21 million people, although officials have not publicly stated whether they believe the Chinese government was responsible.

The highly interconnected nature of the national power grid and the increasing pressure placed on grid reliability by federal and state policies, including the EPA’s recently issued Clean Power Plan and states’ renewable portfolio standards, could exacerbate the impacts of a cyber-attack on energy infrastructure and potentially lead to “cascading blackouts.” Former FERC Chairman Jon Wellinghoff is among those who believe that the solution to preventing cascading blackouts is to move to a system of “micro-grids” that operate independently from one another. The U.S. military is already moving in that direction.

Power generation and delivery are not alone, of course. The oil and gas sectors are inviting targets as well. Some experts say that particular vulnerabilities exist at “single-point” assets such as refineries, storage terminals, and other buildings, as well as “networked features” such as pipelines and cyber systems. Enemies may focus on a large-scale attack with the goal of temporarily halting the supply of oil and gas or even to create an environmental disaster.

Reminiscent of the time after World War One in which the world’s powers were sucked up in the vortex of a naval arms race and in came the Washington Naval Treaty of 1922, today’s superpowers are now doing something similar. President Obama appeared with Chinese President Xi Jinping on September 25 to announce that the United States and China had reached an agreement on a number of issues related to cybersecurity. This U.S.-China agreement comes on the heels of China’s May 2015 cybersecurity agreement with Russia, and China’s recent attempt to enact laws requiring foreign firms operating in China to use China-approved encryption and reveal all source code for inspection, in addition to the OPM breach and DOJ indictments mentioned above. In the agreement, the United States and China agreed to cooperate “with requests to investigate cybercrimes, collect electronic evidence, and mitigate malicious cyber activity emanating from their territory” and “to provide updates on the status and results of those investigations.” To review the timeliness and quality of responses to these requests, both countries have agreed “to establish a high-level joint dialogue mechanism on fighting cybercrime and related issues,” which will include high-ranking Chinese officials, the DHS Secretary, and...
the U.S. Attorney General, along with participation from other agencies. The first dialogue will be held by the end of 2015 and will occur twice per year thereafter.

In addition to this recent agreement, the United States and China are believed to have a framework in place for a cyber-warfare agreement that would prohibit either country from launching an initial cyber-attack on the other’s critical infrastructure during peacetime. One hopes for, but experience shows cannot count on, better success now on cybersecurity than with the Washington Naval Conference.

Additional American domestic efforts to improve national cybersecurity are coming from both the Executive and Legislative branches. Executive Order 13636 requires the National Institute of Standards and Technology, part of the Commerce Department, to create a framework to reduce cybersecurity risk for organizations within critical infrastructure sectors, including the energy sector. The framework, released in February 2014 and updated in December 2014, is based on existing standards, guidelines, and practices. Compliance with the framework, however, is voluntary.

The Department of Energy’s Office of Electricity Delivery & Energy Reliability also focuses on cybersecurity and works with the DHS, industry, and other agencies to reduce the risk of energy disruptions from cyber-attacks. The Office designed the Cybersecurity for Energy Delivery Systems (“CEDS”) program to assist the energy sector asset owners (electric, oil, and gas) by developing cybersecurity solutions for energy delivery systems through integrated planning and a focused research and development effort. CEDS co-funds projects with industry partners to make advances in cybersecurity capabilities for energy delivery systems.

The Department of Energy’s Oil and Natural Gas Subsector Cybersecurity Capability Maturity Model (ONG-C2M2), developed in partnership with the DHS, is an 83-page document that helps improve cybersecurity capabilities and includes reference material and implementation guidance specifically tailored for the oil and natural gas segments of the energy sector. The model can be used to strengthen cybersecurity capabilities in the ONG subsector; enable ONG organizations to effectively and consistently evaluate and benchmark cybersecurity capabilities; share knowledge, best practices, and relevant references within the subsector as a means to improve cybersecurity capabilities; and enable ONG organizations to prioritize actions and investments to improve cybersecurity. The ONG-C2M2 is designed for use with a self-evaluation methodology and toolkit.

Before the Senate now is a bill sponsored by Senate Intelligence Chairman Richard Burr (R-N.C.), S. 754, the “Cybersecurity Information Sharing Act” (“CISA”), which requires the Director of National Intelligence, the DHS Secretary, the Secretary of Defense, and the U.S. Attorney General to create a system to promote the sharing of a broad range of cybersecurity information. CISA is similar to two House bills that passed last April, the “Protecting Cyber Networks Act” (H.R. 1560) and the “National Cybersecurity Protection Advancement Act” (H.R. 1731).

CISA would give private entities, including oil and gas companies, greater liability protection for sharing personal data related to certain cybersecurity information. CISA has faced strong opposition, mainly due to concerns that it may impinge on individuals’ Fourth Amendment right to privacy. If agencies are to store personal information, they must maintain highly sophisticated cybersecurity systems. CISA, however, does not include any requirements or funds to promote these systems. Twenty-two amendments are on the Senate floor, many of which limit the events that provide legal immunity and reduce the ability for agencies to share information with one another. The DHS has expressed concern because the bill allows other agencies to collect this information, potentially reducing the DHS’s current role in this space.

Others have criticized CISA for not going far enough. CISA only creates a framework for information-sharing intended to allow agencies to identify how best to protect against future cyber-attacks. What some expect, or hope, to follow CISA is ultimately the enactment of minimum standards for corporate cybersecurity systems. A vote on the bill is expected soon. A number of Senate and House committees and subcommittees have held hearings on cybersecurity in recent weeks and are
expected to hold further meetings throughout the month. In a statement made before a House committee last month, National Intelligence Director James Clapper stated that the absence of universally accepted and enforceable norms of behavior in cyberspace has allowed cyber-attacks to go undeterred.

Pennsylvania is acting as well, with the PUC in particular showing exemplary leadership. Public utilities are required to develop and maintain a written cybersecurity plan under 52 Pa. Code §§ 101.1-101.7. The PUC took the occasion of its October cybersecurity summit to release its second edition of the PUC Cybersecurity Best Practices for Small and Medium Pennsylvania Utilities. The PUC’s “Cyber Team,” created in 2012, compiled the Best Practices document which is available on the PUC’s website (see http://goo.gl/oMPaae). The document is a magnum opus loaded with information including ways to prevent identity or property theft; how to manage vendors and contractors who may have access to a company’s data; what to know about anti-virus software, firewalls, and network infrastructure; how to protect physical assets, such as a computer in a remote location or a misplaced employee device; how to respond to a cyber-attack and preserve forensic information after the fact; how to report incidents; the potential benefits of engaging a law firm in advance of a breach; and a list of federal cyber incident resources.

Pennsylvania also boasts one of the nation’s top cybersecurity innovators, Eric Avakian, Pennsylvania’s Chief Information Security Officer, who was named a 2015 top 10 “Influencer” by GovInfoSecurity in recognition of his efforts toward improving government IT security policy. Others on the list include members of Congress, leaders of federal agencies, and White House staff.

In light of the enormous asymmetrical physical and financial damage that cyber-attacks can inflict, as well as our apparent vulnerability to those attacks, one thing is clear: a good defense (and perhaps even offense) against such mischief is going to require not only continued efforts, but also an ever-increasing amount of attention, teamwork, effort, and human and financial capital investment going forward.

Reprinted with permission from the October 16, 2015, edition of The Legal Intelligencer © 2015 ALM Media Properties, LLC. All rights reserved. Further duplication without permission is prohibited. For information, contact 877-257-3382, reprints@alm.com or visit www.almreprints.com.

For additional information, please contact:
Michael L. Krancer
215.569.5535 | MKrancer@BlankRome.com
Margaret Anne Hill
215.569.5331 | 202.772.5811 | MHill@BlankRome.com
Thomas M. Duncan
215.569.5642 | TDuncan@BlankRome.com
Frank L. Tamulonis III
215.569.5725 | FTamulonis@BlankRome.com