CYBER-RISK MANAGEMENT

WILL HACKERS CAUSE THE NEXT ENERGY CRISIS?

Sandro Melis • Angelo Rosiello • Silvio Sperzani

Energy companies are suffering from an increasing and unprecedented number of cyberattacks. The most alarming example so far: a malware attack in 2014 that compromised the operations of more than 1,000 energy companies in 84 countries, including the United States, Spain, France, Italy, Germany, Turkey and Poland. This cyber campaign, reportedly waged as a means of industrial espionage, gave hackers the ability to cripple wind turbines, gas pipelines and power plants at the click of a mouse.

For many years, the world has benefited from information technology advances that have improved the productivity of almost every sector of the energy industry – drilling, pipelines, power generation and transmission. But we continue to underestimate the dark side of this equation: Greater dependence on information technology also increases energy companies' risks. A recent *Global Risks* report by the World Economic Forum and its partners (including Oliver Wyman) ranks cyberattacks as one of the top 10 risks most likely to cause a global crisis. The World Energy Council, a forum for energy ministers and utilities, considers cyber threats as one of the top five risks to the world's energy infrastructure.

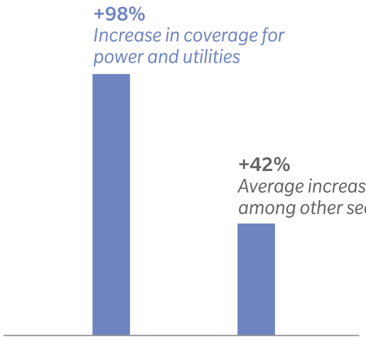
In response, more than 30 countries – including Germany, Italy, France, the United Kingdom, the United States, Japan and Canada – have unveiled cybersecurity strategies. And on June 29, 2015, the Latvian Presidency of the Council of the European Union reached an understanding with the European Parliament on the main principles of what could become a unified directive for the European Union to protect critical infrastructure.

But the searing reality is that both the growing strategic relevance of data and the potential impact of data breaches are outpacing these initiatives. Former chief of the United States' National Security Agency, General Keith Alexander, has commented that countries need something like an integrated air-defense

EXHIBIT 1: RISING CYBER RISKS

Power and utilities companies are spending more on cyber-risk insurance to protect themselves from an increasing number of cyberattacks

PERCENT INCREASE IN INSURANCE COVERAGE



CHANGE IN COVERAGE BY TYPE

Security and privacy coverage	+0%	—
Media coverage	+14%	↑
Regulatory defense coverage	+0%	—
Business interruption coverage	+3%	↑
Information asset coverage	+14%	↑
Cyber extortion coverage	+14%	↑

Note: Percentage increase in spending by companies with more than $1 billion in revenues on cyber-risk insurance from 2012 through 2014
Source: Marsh Global Analytics

system for the energy sector to keep up with mounting cyber risks. Recent clashes between the White House and Republicans over the establishment of a new Cyber Threat Intelligence Integration Center, however, show that marshaling the resources required to protect energy companies more broadly will take time.

98

The percentage increase in cyber insurance coverage by power and utilities firms in the past two years

Meanwhile, cyber risks to the energy industry are becoming more serious and the implications more far-reaching than is commonly recognized. One reason is that the industrial control systems that support energy companies are no longer as sealed off from external threats. Electric utilities depend on automated controls to run their grids, which are managed through interconnected network systems. Oil and gas companies depend on data networks to manage facilities and to interpret seismic developments. Refiners, too, rely on data networks to manage meters and to analyze their customers' needs.

So what can be done? So far, many energy companies have tried to mitigate cybersecurity threats by increasing their spending on information technology solutions, implementing new IT procedures and buying more insurance. Since 2012, energy companies with revenues of more than $1 billion have increased their cyber insurance coverage worldwide by 98 percent, according to Marsh Global Analytics estimates. Marsh, like Oliver Wyman, is a division of Marsh & McLennan Companies. (See Exhibit 1.)

While these initiatives are understandable and laudable first steps, much more needs to be done. Above all, energy companies should treat cyber risks as permanent risks to their entire enterprise and not as isolated "information technology" events. Unlike strategic, operational, and financial risks, cyber risks are often mistakenly treated as lower priorities and relegated to information communications and technology departments. Consider: Computer systems that remotely monitor and control plants and equipment of oil and gas companies and electric utilities are often outside the responsibility of most chief information security officers. Even managers in charge of guaranteeing that these systems are compliant with a company's policies often don't understand their technical specifications.

As a result, the true cyber risk exposure of energy companies often goes unnoticed by top management and boards of directors, leaving the companies at higher risk than necessary. Cyber risks are rarely quantified or linked with their potential impact on companies' financials, making it almost impossible to conduct cost-benefit analyses or to make strategic choices. Information technology departments introduce new technical solutions with minimal top-level direction. Companies adopt case-by-case reactive measures instead of a balanced portfolio of initiatives that involve their entire organization and align with their overall appetite for risk.

As with other operational risks, companies should set a target level of cybersecurity for all of its software, hardware and people based on their importance to the firm's overall appetite for risk. The company should then ensure that controls and processes address gaps that are accordingly prioritized, starting with those that are mission critical. For example, a company might first safeguard its billing and customer relationship management systems since they could put its revenues and reputation

1,000

The estimated number of energy firms that hackers compromised in a global malware attack in 2014

at serious risk if corrupted before addressing risks to video-conferencing tools or internal community portals.

At the same time, top managers in the energy industry need to develop a cyber risk management culture to the point that it becomes as second nature to employees as handling high hazard equipment. Cyber risk management goals should be baked into performance targets, incentives, regular reporting and key executive discussions. When executives evaluate their tolerance for breaches that could impact their company's reputation or violate health, safety and environment standards, cyber incidents involving their industrial control systems should be front and center.

Otherwise, like other slow-building risks that people take for granted, ignoring the threat of increasing cyberattacks could drop unprepared energy companies into the middle of a full-blown energy crisis. This isn't a threat that is going away. Energy companies need to do the math and start making cybersecurity a top priority.

SANDRO MELIS
is a Milan-based partner in
Oliver Wyman's Energy practice.

ANGELO ROSIELLO
is a Milan-based principal in Oliver Wyman's
Energy practice.

SILVIO SPERZANI
is a Milan-based partner in Oliver Wyman's
Strategic IT & Operations practice.

This story first appeared on BRINK.