MARSH

MARSH RISK
MANAGEMENT RESEARCH

ADVANCED CYBER ATTACKS ON GLOBAL ENERGY FACILITIES

MARCH 2014

MARSH GUY CARPENTER MERCER OLIVER WYMAN

MARSH & McLENNAN COMPANIES

CONTENTS

PROTECTING ENERGY FACILITIES AGAINST GROWING CYBER RISKS

For the last quarter of a century, the global energy sector has relied on the protection offered by standalone and closed industrial control systems (ICS) as the primary barrier to the cyber security threat. Today, however, with energy facilities worldwide generally aging, upgrades and expansion projects are ushering in a wave of new ICS and supervisory control and data acquisition (SCADA) systems built on openness and interoperability. While the sector has been quick to take advantage of these new internet-connected systems to reduce cost, improve efficiency, and streamline operations, they have exposed it to a host of cyber security risks that are only just beginning to be understood.

To date, cyber-attacks directed towards the global energy sector have largely been untargeted and data-driven, as companies and individuals have attempted to gain access to personal or sensitive financial data. The nature of the threat is beginning to change, however, and companies across virtually all industry sectors have begun to witness much more intelligent and complex attacks that seek to take charge of ICS in order to inflict damage to property and operations.

In the short term at least, there appears no end in sight to this trend. For as long as attack retains the advantage over defense, cyber-attacks will likely increase in frequency and sophistication, and inflict greater damage to the networks and systems they infiltrate. The pace of this development is alarming. In the two years from 2009 to 2011, for example, General Keith Alexander, the departing N.S.A. director and commander of the United States Cyber Command, said the US catalogued a 17-fold increase in cyber-attacks. In the first six months of 2013, there were more than 800 regulatory filings that mentioned cyber-related risks, representing a 106% increase from the same period in 2012, according to a June 20, 2013 article in The Wall Street Journal.

ENERGY SECTOR TARGETED DISPROPORTIONATELY

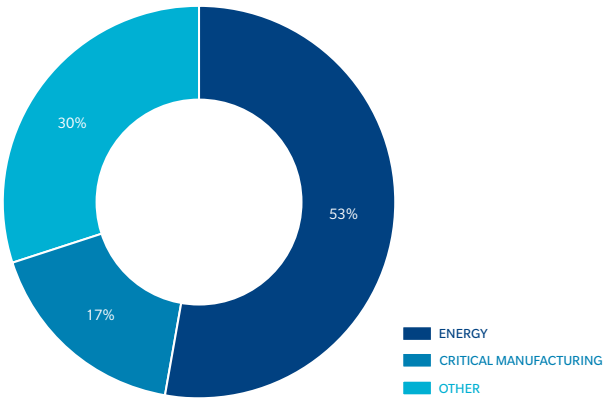
Although the global energy sector has yet to experience catastrophic physical damage to facilities or disruption to supply as a result of a cyber-related event — publicly, at least — the disproportionate rate at which it is targeted for cyber-attacks makes it appear only a matter of time before this trend is broken. According to the US Department of Homeland Security, 53% of the 200 incidents responded to by its Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) between October 2012 and May 2013 were directed toward the energy sector (see **FIGURE 1**). To put that in perspective, the second highest industry was manufacturing, which attracted 17% of attacks.

The energy sector's resiliency to date is certainly not due to a lack of effort on the part of the hackers. In August 2012, the world's largest state-owned oil and gas supplier, Saudi Aramco (officially the Saudi Arabian Oil Company), was the victim of a malicious attack intended to halt the company's crude oil and gas supplies. Although the virus — given the nickname "Shamoon" by investigators — failed in its primary objective, it nevertheless destroyed the hard drives of more than 30,000 desktop computers and 2,000 servers, forcing IT systems to be disconnected from the internet for two weeks.

Computer viruses such as Shamoon and the US-developed Stuxnet virus, the latter of which successfully disrupted uranium enrichment at the Iranian Natanz nuclear facility in 2010, have drawn the energy sector's attention to the potential disruption that could be caused by a malicious piece of software. Developments such as this, together with a general inability to transfer the risk of damage to property resulting from cyber incidents, have led to a high level of concern. A poll included in a 2013 report by Zpryme Research & Consulting revealed that 63% of energy companies were "very concerned" about the prospects of cyber or network attacks; 33% said they were "moderately concerned," with just 5% indicating only "slight" concern.

FIGURE 1 **ICS-CERT INCIDENT RESPONSES — OCTOBER 2012 TO MAY 2013**

Source: US Department of Homeland Security, Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), June 2013



Just as the cyber threat has grown in its complexity, so too have the possible motivations behind the attacks. Whereas cyber-attacks had previously tended to stem from lone hackers, today they may originate from companies seeking to cause disruption to a rival's operations in the hope of gaining competitive advantage; or from cybercriminals intending to benefit from resulting commodity price fluctuations due to restricted supply; or from a rogue government as part of cyber warfare campaigns to damage or disable critical infrastructure. There is also the threat from insiders with high-level access to increasingly complex and pervasive computer networks.

INTERNET-BASED ICS: BACKDOORS FOR HACKERS

The cyber threat towards the energy sector is not new. Exposures have generally been born out of a combination of flaws in design and operation, which were historically driven by safety and efficiency; security was simply not an issue. This same reasoning can generally be applied to risk management at energy facilities, which has traditionally centered on ensuring process safety on the one hand, and protecting confidential proprietary data on the other, with little attention paid to the security of the ICS.

Even with closed systems, there is always the risk of internal recklessness or sabotage — several US power plants have previously been infected by USB stick malware attacks, for example. Yet the separation of industrial and business systems through the use of firewalls and other means has so far — in the energy sector at least — restricted any disruption resulting from the internal uploading of malicious software to commercial and management functions (as was the case with Saudi Aramco).

The adoption of more modern, internet-based ICS and SCADA systems has been widespread in recent years as companies have sought greater business insight, remote access, and interoperability between systems. Unlike past industrial control systems, which were closed and predominantly exclusive to respective operating companies, these new systems have integrated control systems with other information technology networks, providing malicious persons with the opportunity to gain access to a facility's IT software without needing to be onsite. Once inside the system, an infiltrator could, in theory, open an ESD valve, or adjust alarm system settings at a gas or petrochemical plant, for example, leading to fire or explosion and, consequently, damage to property, environmental harm, and loss of life.

Although the energy sector has yet to experience catastrophic physical damage or a business interruption (BI) loss as a result of a cyber-attack, several external attacks on similar "open" ICS have been witnessed against utilities, indicating a worrying trend. But unlike for utilities companies, a cyber-attack on computer control or emergency shutdown systems, even at a small refinery, or petrochemicals or gas plant, could result in estimated maximum loss (EML) as a result of fire or explosion worth hundreds of millions of dollars. Even if the damage resulting from an attack were localized, BI values could potentially run into the billions of dollars as the wait for long lead time components stretches into years as opposed to months. The variance in loss estimates differs much more greatly between offshore assets; complete loss of a platform could be anything from tens of millions of dollars to more than one billion, with BI at the top end running into several billions of dollars for every 12 months of lost production.

The risk is accentuated for new projects, which, more often than not, have led to greater levels of complexity and higher value concentration. While new projects generally incorporate more sophisticated risk management practices and apply rigorous standards to minimize risk, heightened ICS security risks exist at the beginning and end of facility projects, similar to classic equipment reliability (see **FIGURE 2**).

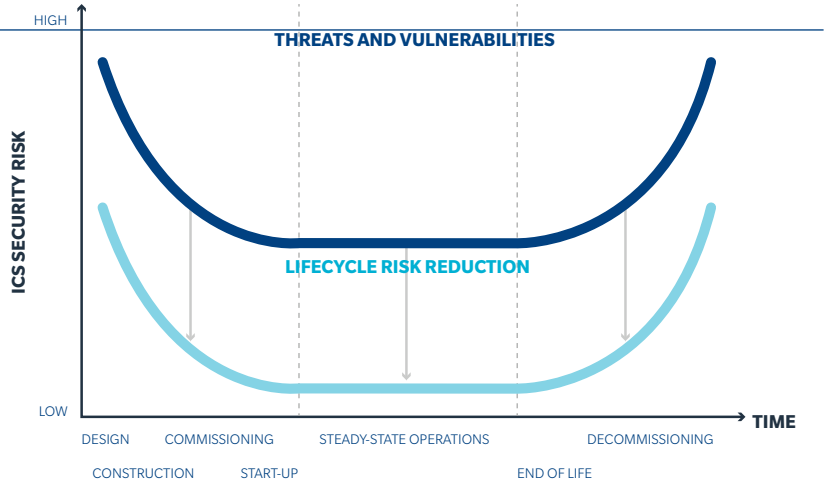


FIGURE 2 | **ICS SECURITY RISK RELIABILITY BATH-TUB CURVE**
Source: Marsh

THE COVERAGE GAP

While cyber policies are available to provide protection against BI arising from cyber-related disruption, cyber-attack has been a standard insurance policy exclusion since 2003, with most markets using CL380, which states:

> ...in no case shall this insurance cover loss damage liability or expense directly or indirectly caused by or contributed to by or arising from the use or operation, as a means of inflicting harm, of any computer, computer system, computer software program, malicious code, computer virus or process or any other electronic system...

Notably, the CL380 exclusion was inserted into most property policies without any such losses occurring. To this day, the energy sector has yet to experience catastrophic physical damage to facilities or operations that has been attributed to a cyber-related event. In an ideal world, these exclusions would be gotten rid of; however, the argument from underwriters when asked to consider the removal of the CL380 clause is that the exclusion is routinely imposed upon underwriters themselves by their treaty reinsurance.

As such, any solution to fill this gap in cover will most likely be addressed by a standalone product, and there is a real opportunity for innovative carriers to develop and market a solution to enable risk managers to transfer this unique type of risk.

While any new product would understandably start with more limited cover and capacity than the total exposure many energy clients may have to cyber attack — which could feasibly run into billions of dollars for the largest sites — it is not difficult to foresee the market developing in a similar manner to that of the cyber liability market, which today has annual premiums in excess of US$500 million after being only a few years in existence.

COLLABORATION REQUIRED TO IMPROVE RISK MANAGEMENT

Although insurance is vital to mitigate the impact to energy companies' bottom lines, the nature and changing risk profile of the cyber threat — from economic espionage to causing disruption of production — demands a collaborative, risk-based approach from businesses and governments around the world.

In the US, the Obama administration's new Cybersecurity Framework has sought to define a common set of security standards for a list of 16 defined critical infrastructure sectors, including standards and approaches for ICS. In Europe, meanwhile, the EU is close to finalizing its own cybersecurity directive to reduce the cyber threat posed to critical infrastructure, communications, and public services. The aims of these two pieces of legislation are broadly similar: to encourage businesses to adopt rigorous risk management practices commensurate to the threat at hand, and share information on the changing risk profile, thereby increasing awareness.

Initiatives such as these — based on information-sharing and cooperation — will go some way in the battle against cyber attackers, and are the first step towards overturning the underlying dynamic in favor of the defense. The next and much more difficult challenge will be to identify common vulnerabilities before assessing the potential impacts of cyber risk to the energy sector — particularly from an economic perspective — at individual business, national, and international levels. Until then, it is imperative that energy companies consider the risk of cyber-attack as an inevitable one, and focus on preparing scenarios to identify, respond, and contain any attacks accordingly.

ABOUT MARSH

Marsh is a global leader in insurance broking and risk management. We help clients succeed by defining, designing, and delivering innovative industry-specific solutions that help them effectively manage risk. We have approximately 27,000 colleagues working together to serve clients in more than 100 countries. Marsh is a wholly owned subsidiary of Marsh & McLennan Companies (NYSE : MMC), a global professional services firm offering clients advice and solutions in the areas of risk, strategy, and human capital. With more than 54,000 employees worldwide and approximately $12 billion in annual revenue, Marsh & McLennan Companies is also the parent company of Guy Carpenter, a global leader in providing risk and reinsurance intermediary services; Mercer, a global leader in talent, health, retirement, and investment consulting; and Oliver Wyman, a global leader in management consulting. Follow Marsh on Twitter @Marsh_Inc.

ABOUT MARSH'S GLOBAL ENERGY PRACTICE

Marsh's Energy Practice is at the forefront of advising energy companies on risk and insurance issues impacting operational success. Our network of more than 350 energy specialists is globally coordinated from 13 strategic hubs. We manage more than US$2.5 billion of insurance premiums in the energy markets on behalf of more than 2,000 clients. Our wealth of expert knowledge is augmented by market-leading risk engineering, project risk management, and claims advisory services.

MARSH

For further information, please contact your local Marsh office or visit our website at marsh.com

BOB PARISI
Network Security & Privacy Practice Leader
+1 212 345 5924
robert.parisi@marsh.com

STEPHEN WARES
EMEA Leader – Cyber Risk Practice
+44 207 357 5420
stephen.wares@marsh.com

GUY BESSIS
Managing Director – Energy Practice
+971 4 212 9128
guy.bessis@marsh.com

PAUL NICHOLSON
Managing Director – Energy Practice
+44 207 357 5579
paul.t.nicholson@marsh.com