Could Energy Industry Dynamics Be Creating an Impending Cyber Storm?

Energy executives are becoming more concerned about the impact a cyber-attack could have on their organization, but greater understanding, quantification, and mitigation strategies may be needed to tackle this growing risk, a recent Marsh survey has revealed.

As the energy industry grapples with economic challenges of the past few years, the wide range of effects a cyber-attack could have on an organization, including the possible impact of business interruption, has been weighing on energy executives' minds.

In a recent survey,[1] conducted by Marsh in partnership with Microsoft, 76% of energy executives cited business interruption (BI) as the most impactful cyber loss scenario for their organization. This highlights not only the growing threat cyber presents for the energy industry, but also the increasing effect any business interruption could have on production and revenues. Meanwhile 23% also cited contingent business interruption (CBI) as one of the most concerning loss scenarios.

A cyber-attack causing BI or CBI has the potential to cause large losses in the industry, particularly given current market trends. After the downturn in oil and gas prices from 2014, many oil and gas companies have been looking at ways to optimize their organizations and make cost-cutting decisions. As a result, the impact of a cyber event causing BI could have an even greater effect than before.

After all, as Marsh mentions in our recent report, *Rethinking Business Interruption Risks in an Optimized Oil and Gas Industry*, many players in the oil and gas sector have been looking for ways to streamline their operations, often resulting in supply chains becoming more integrated and interdependent. If one part of a supply chain was interrupted as a result of a cyber-attack, it carries the potential for devastating consequences across the entire chain.

BI also emerged as the top concern across all of the industries surveyed. As the Marsh/Microsoft report points out, this could also be due, in part, to the complex nature of business interruption itself. While the cost associated with a breach of personal information can be estimated based on historical data, cyber BI costs are more difficult to project because they depend on such factors as the sophistication of the attack, the organization's business model, the level of planning and investment made before the attack, and the organization's response.

INTERCONNECTED SYSTEMS IN THE ENERGY INDUSTRY INCREASE CYBER VULNERABILITIES

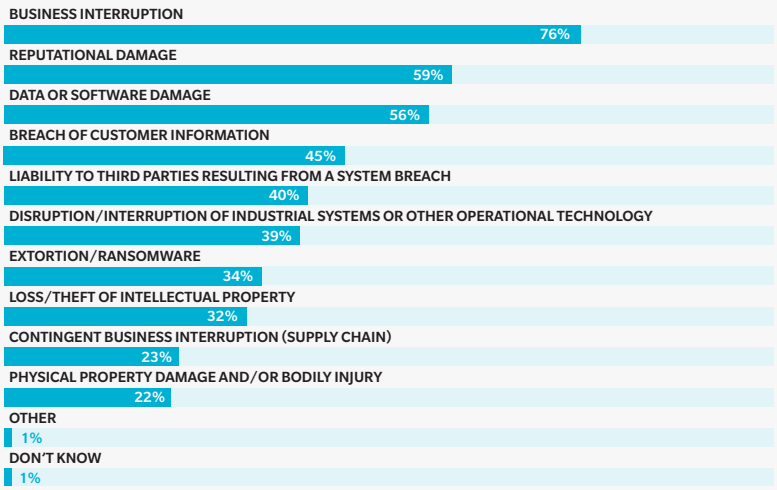
But not all cyber loss scenarios were similarly cited by both energy executives and the larger pool of respondents. One noticeable difference was that energy executives were more likely to identify physical damage as the cyber-loss scenario that could have the greatest impact on their organization, with 22% citing this risk, compared to just 9% of the overall respondents. They also expressed concern that a cyber-attack could disrupt/interrupt industrial systems or other operational technology (39% of energy executives compared to 29% of the overall respondents).

As the energy sector systems that monitor and run operations become more interconnected from smart grids, smart devices, and the growing internet of things, it increases the risk that a cyber-attack could result in physical damage.

Industrial control systems (ICS) are being increasingly linked to the internet and to enterprise business networks, which has opened these systems up to the risk of cyber-attacks, such as malware. This has exposed these systems to new vulnerabilities that have the potential to result in traditional risks such as fires, explosions, machinery breakdown, damage to infrastructure, and more.

As mentioned in a report[2] prepared by Marsh & McLennan Companies, Swiss Re Corporate Solutions, and the World Energy Council, the energy sector should be particularly concerned with these risks. "An attack on energy infrastructure has the potential to cross from the cyber realm to the physical world – a cyber-attack could cause, for instance, a massive operational failure of an energy asset. Large centralized infrastructures are especially at risk due to the potential "domino effect" damage that an attack on a nuclear, coal, or oil plant could cause," the report noted.

FIGURE 1 **Which cyber loss scenarios present the greatest potential impact to your organization?***
Source: Marsh-Microsoft Cyber Perception Survey

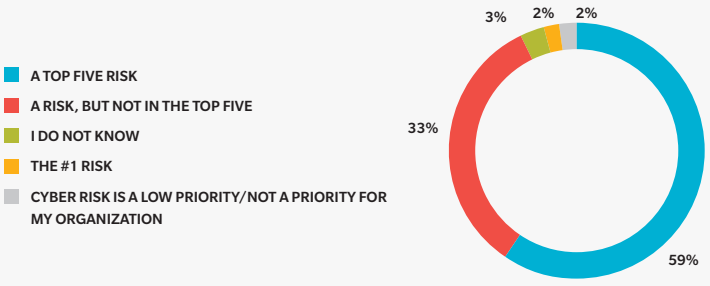


*More than one response allowed

ARE ENERGY ORGANIZATIONS DOING ENOUGH TO UNDERSTAND CYBER EXPOSURES?

Given the economic challenges the industry faces, along with its unique risk profile, it perhaps does not come as a surprise that the majority of energy executives are giving cyber risks some serious thought. The survey revealed that 61% place cyber in the top five risks, or indeed the top risk, faced by their organizations.

FIGURE 2 **Among my organization's risk management priorities, cyber risk is:**
Source: Marsh-Microsoft Cyber Perception Survey



Despite naming this risk as a priority, more than half (54%) of energy executives have not quantified or did not know what their worst possible loss exposures could be. But, with the pace of technological change continuing to rapidly evolve the way the energy industry operates, and physical damage being a risk of concern, these could be extensive. Could we soon see the losses from a cyber-attack equal to that of one of industry's biggest losses, such as Piper Alpha or Deepwater Horizon?

FIGURE 3 For each of the following, please indicate your confidence in your organization's ability to:
Source: Marsh-Microsoft Cyber Perception Survey

Perhaps more worryingly, 26% of energy executives surveyed said they were aware that their company had been victim to a successful cyber-attack in the past 12 months, but, as many cyber-attacks often go undetected for some time, there is a possibility that the actual percentage is higher.

Meanwhile, over half of energy industry respondents said they felt fairly confident in their ability to understand (59%), mitigate (69%), and manage (64%) a cyber-attack. But with some expressing no confidence in their organizations' abilities to address cyber risk, it is clear more work is needed in the energy industry to address these vulnerabilities.

The majority of energy industry respondents seem ready to do just that. After all, 77% of energy executives surveyed said they expect their organizations will increase levels of investment in cyber risk management. In addition, 26% plan to purchase or increase their cyber insurance, while 20% already have insurance in place. Of those that already purchase cyber insurance, one quarter said they planned to broaden and increase the number of risks covered. This likely reflects a desire to prepare for evolutions in technology in the industry such as the internet of things and artificial intelligence, as well as regulatory developments governing data use and breach notifications.

The digitalization of the energy industry is expected to continue. But, as the industry relies more on interconnectivity, the potential for cyber-attacks to cause severe disruption to operations, loss of data, and financial losses should remain a key concern for energy executives. For those that have not put plans in place to mitigate and manage attacks or have not measured their cyber exposure, now is the time to prepare for the impact an attack could have on operations and systems.

As the industry relies more on interconnectivity, the potential for cyber-attacks to cause severe disruption to operations, loss of data, and financial losses should remain a key concern for energy executives.

1. Marsh. *By the Numbers: Global Cyber Risk Perception Survey,* available at https://www.marsh.com/uk/insights/research/global-cyber-risk-perception-survey.html, accessed 1 March 2018.
2. World Energy Council. *The Road to Resilience 2016: Managing Cyber Risks,* available at https://www.marsh.com/uk/insights/research/the-road-to-resilience-2016-managing-cyber-risks.html, accessed 1 March 2018.

ABOUT THE SURVEY

This report is based on findings from the *Marsh-Microsoft Global Cyber Risk Perception Survey* administered between July 2017 and August 2017. Overall, 1,312 senior executives participated in the global survey, representing a range of key functions, including information technology, risk management, finance, legal/compliance, senior management, and boards of directors. Energy industry executives made up approximately 7% of the total respondents.

CONTACTS

ANDREW HERRING

Managing Director & Practice Leader, Energy
+44 (0)20 7357 5589
andrew.herring@marsh.com

AMY BUTTERWORTH

Client Executive
+44 (0)20 7357 5061
amy.butterworth@marsh.com