

October 22, 2013

The New Energy Landscape: What Leading Companies Need to Know

Booz Allen Announces Top Six Oil and Gas Industry Trends for 2014

MCLEAN, Va.--(BUSINESS WIRE)-- Today's oil and gas industry executives — including control room operators monitoring use data, chief information security officers analyzing the potential cyber security risks of a new IT system, and oil rig managers discussing drilling sites with geologists — are making business decisions in an interconnected landscape of risks and rewards. Success demands balancing the dizzying array of new regulations, cutting edge technology, and emerging threats and opportunities that are ever present in this industry.

"Partnering with our oil and gas clients, we examine the near and long-term trends for this industry, and it is striking to see how regulation, the cyber threat environment, and internal challenges are converging to shape the path forward," said Emile Trombetti, senior vice president, Booz Allen. "It is critical that industry leaders consider how these trends provide challenges and opportunities for their organizations that can ultimately help them better prioritize and meet their strategic and business goals."

Booz Allen Hamilton has identified the six key trends that are poised to greatly impact the oil and gas sector of tomorrow, and that what every oil and gas executive needs to know today.

Top Six Energy Industry Trends for 2014:

1. The technology supply chain will increase the need for cyber risk management. Oil and gas companies recognize that embracing networked infrastructures allows them to more efficiently operate their business, and in doing so, they increasingly rely upon vendor materials, products and services. However, the industry is only now coming to terms with the cyber risk management challenges created by a more open network and increased reliance on the technology supply chain. Oil and gas leaders must address the weighty task of assessing the security of third-party vendors and protecting critical business assets from those who should not have access or who wish to disrupt the business.
2. Cyber risk management will become more customized. Every oil and gas company stands to be hacked, and only so much can be done to thwart this threat. Companies must create unique approaches to minimize the impact of an attempted attack, and protect critical assets. In particular, oil and gas companies need to focus on developing comprehensive security risk management plans tailored to the circumstances when entering high-risk environments, such as ventures into new geographic locations, markets and products.
3. Future competitive advantages depend on technological innovation. Until recently, oil and gas companies did not innovate beyond what was required to pull resources out of the ground with a reasonable amount of success. However, there has been a noticeable shift as companies begin to view technology as a new frontier for competitive advantage.

Oil and gas companies are using the latest ideas, such as mobility, cloud computing, and knowledge management, and wrapping them around their current processes to make everything work better. However, as innovation takes off, companies must turn their attention to protecting the R&D that went into creating this intellectual property, which creates another layer of security that must then be implemented.

4. Striking the right balance between strong cyber risk management and regulation will become more challenging. Regulations help companies secure themselves from cyber threats. However, regulations apply a one-size-fits-all method to security that does not take into account each company's "attack surface," the unique vulnerabilities that come with its specific business processes. Often there are competing priorities between addressing what is required by regulation and what is genuinely needed at the time to effectively protect the company's systems from cyber intrusions.

Also, firms must always stay abreast of the constantly changing regulatory environment. Just as energy companies achieve compliance under current regulations, new regulations are developed. Oil and gas companies must balance a host of issues, such as compliance with environmental regulations, while balancing geopolitical issues that can have material impact on the bottom line.

5. An aging workforce is creating unique risk management, infrastructure, and HR challenges. The oil and gas industry is facing a shrinking talent pool for those with specialized expertise. Most individuals who have the institutional and

technological "know how" about their organization's specific cyber risks and operations are looking toward retirement. This creates a knowledge gap that younger employees cannot meet on their own, and requires oil and gas leaders to work across their business to capture, retain, and integrate human capital intelligence. According to Ernst & Young, nearly 90 percent of senior human resources executives at 22 top international oil and gas companies believe their industry faces a talent shortage and call the problem one of the top five business issues facing their companies.

6. Data will continue to create differentiators. Oil and gas companies are facing an explosion in the amount and types of data that their assets generate, yet they risk being less competitive if they do not make this data work for them. Organizations must also understand that while their data presents business opportunities, it also raises certain challenges. For example, industry leaders must determine how to analyze and present their data in a way that allows the firm to create action, both in terms of driving business strategies and in understanding anomalies associated with their critical assets.

A recent ABI Research study predicted that cyber attacks against oil and gas infrastructure will cost companies \$1.87 billion by 2018: "Cyber Risk Management is now a Board level risk that every company involved in Oil and Gas production must address. Wherever there is an intelligent device, whether it be a complex set of devices controlling a oil platform, or even a simple device that controls the opening and closing of a valve on the pipeline, they could be at risk of being controlled by an unauthorized entity. Oil and Gas executives are becoming more resigned to the fact that much more must be done in executing an effective cyber risk management program."

Booz Allen works with a variety of oil and gas industry firms to provide a carefully curated set of solutions that help them gain a competitive advantage and manage a wide spectrum of issues. For example, Real Time Analytics resources better inform capital project management programs and help companies determine where and when to invest. Booz Allen's industry expertise gives oil and gas companies access to a diverse array of institutional experts around the world who understand the clients' unique challenges and opportunities.

About Booz Allen Hamilton

Booz Allen Hamilton is a leading provider of management consulting, technology, and engineering services to the U.S. government in defense, intelligence, and civil markets, and to major corporations, institutions, and not-for-profit organizations. Booz Allen is headquartered in McLean, Virginia, with a MENA headquarters in Abu Dhabi, employs more than 23,000 people, and had revenue of \$5.76 billion for the 12 months ended March 31, 2013.

BAHPR-GI

Booz Allen Hamilton
Media Contact:
Carrie Lake 703-377-7785
Lake_Carrie@bah.com

Source: Booz Allen Hamilton

News Provided by Acquire Media