IADC Briefing Book
Cybersecurity

Cybersecurity is a growing concern in the oil and gas industry. For the past 30 years, the oil and gas sector has been targeted by cyberattacks, including the well-known 2012 attack on Saudi Aramco, which crippled 30,000 computers and disrupted corporate operations for months – although it did not disrupt production. Cyber risks affecting the digital oilfield include wireless offshore technologies and automated drilling assets and drilling control systems. [1]

Key Messages

- According to the U.S. Department of Homeland Security, the energy sector is one of the greatest targets for cyber threats. [2] Innovations like big-data analytics, digital technologies and remote operations have offered dramatic advancements in optimization and efficiency. However, these come with associated cybersecurity risks, and industry takes the risks very seriously.
- A cyberattack has the ability to disrupt a company's operations and have a negative impact on their reputation, shareholder confidence and/or stock price.
- Oilfield service companies, operators and asset owners are taking a proactive approach to mitigate security, regulatory and litigation risks by evaluating and investing in cybersecurity risk management as part of their overall risk management programs. These include incorporating cybersecurity vulnerability assessments, an evaluation of liability and indemnification and information sharing provisions specific to cybersecurity incidents in service contracts. [1]
- The oil and gas sector continues to invest in cyber and data protections. Many companies have put in place contingency plans for a cyber attack or compromise that incorporates legal, marketing/PR, regulatory and compliance and cyber response teams expertise.
- In recognition of the critical importance of cybersecurity to drilling operations, in 2016 IADC's Cybersecurity Subcommittee wrote the IADC Guidelines for Assessing and Managing Cybersecurity Risks to Drilling Assets. The guidelines are the only cybersecurity guidance to specifically address drilling operations and draws from international standards to provide a means to assess the risk to drilling rigs from cyber attacks. [3]

Resources

1. Rigzone:http://www.rigzone.com/news/oil_gas/a/136434/Report_Oil_Gas_Cybersecurity_Risks_to_Continue_in_2015/?pgNum=1
2. Homeland Security Today: http://www.hstoday.us/single-article/dhs-cyber-attacks-on-us-critical-manufacturers-on-the-rise/28802bd3d10b6ddbd7bf2f34ef3e4e6c.html
3. IADC Cybersecurity Guidelines. http://www.iadc.org/ebookstore/ebook-iadc-guidelines-assessing-managing-cybersecurity-risks-drilling-assets/