Fundamentals of petroleum energy and mitigating global cybersecurity attacks rese...

Business, Company

Homeland Security and Technology

Fundamentals of Petroleum Energy & Mitigating Global Cyber security Attacks

Commentary 1 Homeland Security the Fundamentals of Petroleum Energy

I agree with the comment that exploration is the most critical component of the petroleum sector because it initiates gas extraction. Aside from this there is a possibility that federal, state

and local government rules may be violated as they deal with environmental issues during gas operations in order to safeguard water resources. Unlike refining or distribution, these two components of the process of gas exploration only take over the initial work laid down during the exploration activity. This can be illustrated in the recent Arctic exploration where the competing states are vying to locate the 13 percent of oil reserves and 30 percent of natural gas reserves Ernest and Young, 2013). Another evidence to justify that exploration is critical is due to the fact that it may cover substantial political and jurisdictional issues of the competing nations.

Commentary 2 Mitigating Global Cyber security Attacks on the Enterprise

I agree with the answers provided that cyber security policies should be implemented in order to prevent cyber attacks in a global perspective. Every company must enforce policies that will examine and monitor all new software and hardware installed into the network, particularly those that originate from foreign vendors or entities. The training and awareness policy is also vital in order to educate the employees on topics such as spear-

phishing, e-mail protocols and social networking protocols of the company's network. By enforcing strict policies, it will prohibit the installation of malicious software on or unauthorized access to the network systems of the company or firm. Thus, despite efforts of the hackers to break into the system using their sophisticated methods and technical skills, preventive measures should be implemented in order to strengthen the system security plan of each company, firm or agency.

References:

Ernest & Young. (2013) Artic oil and gas. Retrieved on June 2, 2013, from http://www. ey. com/GL/en/Industries/Oil---Gas.

Lebanidze, E. (2011). Guide to Developing a Cyber Security and Risk Mitigation Plan. Wilson

Boulevard, Arlington: National Rural Electric Cooperative Association.

Rudolph, K. (2009). " Implementing a security awareness program". In S. Bosworth, M. Kabay,

& E. Whyne (Eds.), Computer Security Handbook, 5th ed. Hoboken, NJ: John Wiley &

Sons, Inc.

Snow, G. (2011). Testimony: Statement Before the Senate Judiciary Committee, Subcommittee

on Crime and Terrorism. Retrieved on June 2, 2013, from

Federal Bureau of Investigation: http://www. fbi.

gov/news/testimony/cybersecurity-responding-to-the-threat-of-cyber-crime-and-terrorism.