Oil and Gas Cyber Security North America

13-14 May 2015, Houston, Texas, USA

In the run up to the conference, we asked our featured speakers a few questions about current challenges and opportunities in the cyber security market.

Q AND A WITH **THOMAS RUSSO**, SENIOR INDEPENDENT ENERGY ANALYST

In his presentation entitled "Oil & Gas Cyber Security – Not Just About Information Risk" Mr. Russo will discuss the physical ramifications of a cyber-security breach on the different entities within the oil and gas supply chain and refocus risk assessment back to the physical commodities prevalent within this sector.

SMi: We have observed quite a dramatic fall in the oil price. With budgets being squeezed, do you believe that Oil and Gas companies are more vulnerable to cyber-attacks now than ever?

T.R.: *The decline in oil prices is affecting capital expenditures especially on oil and wet natural gas shale plays in particular. One large gas producer is reducing its 3-year investment plan expenditures by 27% in response to plummeting oil prices.*

The silver lining in this is that all oil and gas companies are being forced to take a harder look at their assets and to identify the best performers and critical assets. If companies direct their cybersecurity measures at these critical assets, their overall physical and cybersecurity risks may be enhanced.

SMi: In your opinion, are we sufficiently equipped to face the aftermath of a major cyber-attack on an oil and gas company?

T.R.: *In cases where cyber-attacks focus on information alone, most oil and gas companies are equipped to deal with an attack. However, when a cyber-attack disrupts the industrial control systems that govern drilling, gathering, and processing/refining and transportation of natural gas, crude oil or refined petroleum products via pipelines, rail and LNG vessels, companies may not be equipped to deal with the situation.*

Good examples are oil and natural gas pipeline leaks and compressor/pump station disruptions that interrupt supplies. In those situations, oil and natural gas companies will have to rely on disaster recovery plans that have been integrated with state and local governments to protect the public and the environment.

Oil and Gas Cyber Security North America

13-14 May 2015, Houston, Texas, USA

In the run up to the conference, we asked our featured speakers a few questions about current challenges and opportunities in the cyber security market.

SMi: How highly do companies prioritise cyber security within the frame of your business risk strategies?

T.R.: *Unless an oil or gas company understands the business impacts that physical and cybersecurity threats can have on their ability to deliver products to customers and earn revenue, they are probably not prioritizing cybersecurity.*

This is a difficult question that depends both on the type of oil and gas company, actual physical assets owned, and the company's prior experience with cyber and safety events.

For example, an LNG Terminal owner may have little choice except to place a high priority on physical and cybersecurity as a result of federal and state requirements about safety and possible impacts to local communities. In contrast, oil and natural gas pipeline and distribution companies that have little experience with oil or gas leak and catastrophic environmental and safety impacts may do the bare minimum. While some may even believe that attackers have little knowledge of their company's existence and down play physical and cyber security's importance.

SMi: In relation to other sectors, how well do you believe the oil and gas industry has responded to the new threat from cyber-attacks?

T.R.: *The oil and gas industry has always been progressive with respect to technology and safety in delivering products and services. I believe that both industries have taken advantage of existing Federal information sharing of threat information and will continue to be open to innovative and cost effective ways of minimizing risks, especially if they are not compliance driven as they are in the electricity sector.*

SMi: Where do you believe the greatest threat from a cyber-attack lies?

T.R.: *The greatest threat from a cyber-attack will come from individuals or organizations that recognize the economic importance of the oil and gas supply chain and reliance of the electric sector on natural gas. In addition, natural gas, oil and liquid petroleum liquid (LPG) pipelines rely on compression and pumping stations powered by electricity.*

Oil and Gas Cyber Security North America

13-14 May 2015, Houston, Texas, USA

In the run up to the conference, we asked our featured speakers a few questions about current challenges and opportunities in the cyber security market.

Finally even minor cyber-attacks that temporarily disrupt the flow of natural gas, oil and LPG don't have to cause dramatic changes to the supply chain to adversely affect both physical (cash) and energy futures/swaps markets.

SMi: Do you believe the current level of technology and expertise available is adept at detecting disruptions to oil and gas processes brought on from a cyber-attack?

Many cybersecurity technologies can detect changes to oil and gas industrial control processes and associated corporate information systems. However, they place the burden of determining false positives from actual threats on company's IT staff or outside experts who may not be able to respond in a timely manner.

I'm encouraged by new emerging technologies in the marketplace that protect an entire computer system from being attacked and rely on the one-time pad derived by Vernam cipher to encrypt data for all users. In such an ecosystem, even if company assets are lost or compromised, an attacker will not be able to read the information.