**Publication**: Infosecurity Magazine
**Date**: 04.09.2019
**URL**: https://www.infosecurity-magazine.com/opinions/secure-oil-gas/
**Title**: Keeping Data Secure in the Oil and Gas Industry
**Author**: Jerry Askar Managing Director Middle East, Levant & Africa, Certes Networks

# Keeping Data Secure in the Oil and Gas Industry

By Jerry Askar Managing Director Middle East, Levant & Africa, Certes Networks

As automation continues to evolve, the utilities sector is finding that encryption of their network data is a critical to safeguard against cyber-attacks. As organizations across the globe continue to prioritize cybersecurity, the threat landscape continues to expand. Although good progress is being made, it is evident that critical network vulnerabilities are still being left unprotected.

This is particularly the case in the oil and gas sector, which is the latest to enter the cybersecurity spotlight according to the latest threat report by security firm Dragos, which highlighted that the sector is a valuable target for adversaries seeking to exploit industrial control systems (ICS) environments.

The report revealed a new activity group targeting the industry, bringing the total number of tracked ICS-targeted activity groups to nine, five of which directly target oil and gas organizations. What's more, the increased deployment of automation within the oil and gas industry to manage costs, extract the most value from current assets and maximize up-time, only causes the threats to ICS and supervisory control and data acquisition (SCADA) networks to rise.

The threat is clearly high, as are the potential consequences of a cyber-attack on this sector. An attack on an oil or gas organization would not only have severe political and economic impacts, but it would also have a direct effect on civilian lives and infrastructure. Much of how the population lives and works is dependent upon the energy from oil and gas production, from communication, the use of electronic devices and appliances, and even heating, cooling and cooking. The smallest attack on this sector could result in devastating effects.

Beyond consumer impact, an oil or gas company hit by a cyber-attack could experience a plant or production shutdown, utilities interruptions, equipment damage or loss of quality, undetected spills and of course safety measure violations. For example, in December 2018, Saipem, an Italian oil and gas industry contractor, fell victim to a cyber-attack that hit servers based in the Middle East, India, Aberdeen and Italy, which led to the cancellation of data and infrastructures.

**Mitigating cyber-attack damage**

Understanding not just the threats faced by this sector, but also how the attacks are taking place and the behaviors and capabilities of activity groups targeting oil and gas companies, is essential. As the Dragos report warned, there is currently limited visibility – or observability --into the network ecosystem, including communications to and from operations centers, distribution substations and even home "smart grid" networks. This means that intruders can dwell for longer and the root cause of the attack can remain undetected. As is widely documented, the longer an attacker remains in a network, the more damage the breach will cause.

To protect data in ICS/SCADA environments, organizations in the oil and gas industry need an encryption solution that not only safely encrypts data enterprise-wide, but that is also scalable and easy to implement, without disrupting, replacing or moving the network infrastructure. Furthermore, some encryption technologies will provide organizations with greater visibility of their data to monitor deployed policies.

By defining and deploying policies and keys based only on which users should have access to what data, organizations can ensure that only those who need to send or receive the data have the access to do so. In addition, many observability network features can provide crucial flow data so that IT operators can observe policy enforcement and quickly shut down a policy if compromised to stop further damage and potential escalation.

**Conclusion**

Lessons need to be learned from the past attacks on the oil and gas industry, such as the Saipem attack which had global consequences. With the sector facing such a high cyber risk, it's more crucial than ever for oil and gas organizations to inhabit a cybersecurity culture and move from reactionary to proactive.

This means employing an encryption management solution, along with the right forensic intelligence tools, to understand and safeguard against future cyber-attacks and their potential for devastating consequences.

---