NTT Security

Global Overview

Cybersecurity Expertise in the Oil & Gas Sector

The threat of cyber attack hangs over the world's oil and gas fields. Whether onshore, offshore, conventional or unconventional, oil and gas producers now face the same vulnerabilities menacing other major industries.

There was a time when the systems linking oilfield process equipment and control systems were physically separate from traditional IT networks. The growth of mobile technology for field engineers, and the benefits of data collection and analysis, mean everything is now connected to the internet. Upstream management and accounting processes are increasingly digitalized – leaving exploration and production (E&P) companies exposed to network-related vulnerabilities.

The consequences of a cyber attack can be both financial and reputational. If production is halted, income is lost. If partners and suppliers lose confidence in your operational stability, that can make it harder to negotiate new deals. And depending on lease agreements and contracts, there may well be penalties if the flow of oil and gas from a well or lease is disrupted.

In the face of growing attempts to breach defenses, oil and gas producers need to understand the scale of current risk and determine the best response. The SCADA-based systems that monitor devices at the wellhead are a prime target for hackers, and must be well protected. Moves to cut costs in the face of lower oil prices have hastened the adoption of internet of things (IoT) technology – yet many IoT devices lack appropriate security measures.

To keep the oil and gas flowing, upstream companies need to step up their cyber readiness.

Cybersecurity challenges in the upstream oil and gas industry

With digitization on the rise, and cyber criminals often one step ahead of the security learning curve, the oil and gas industry faces a growing number of security threats. These include:

- Attacks on SCADA-based industrial control software, halting or disrupting production
- Malware infection via the extended attack surface, created by the adoption of IoT devices
- A continuing shift from proprietary software to mass-adoption, internet connected products with known vulnerabilities and exploits
- Highly sophisticated, weaponized malware developed and deployed covertly by nation-state actors
- A constantly changing threat landscape with new threats emerging and existing ones becoming more sophisticated
- Increasing number of mobile devices on utility companies' corporate networks, including personal and those used by field personnel

Onshore wells, offshore platforms, and oil and gas pipelines all feed into or constitute the energy companies' critical infrastructure. This and the systems that ensure an organization's efficient operation deserve full cyber protection.

Our unique capabilities

At NTT Security we offer energy organizations a broad range of managed security, risk and compliance services. Our experts have global reach and local resources and understand the specific challenges upstream companies are grappling with at both a global and regional level.

> **"The oil and gas industry is the second most susceptible to cyber attacks, with the potential to cause unprecedented damage and unrest across the world."**
>
> – Brian Lord, OBE; former deputy director, GCHQ

Working with a network of trusted partners and NTT Group companies, we enable your cyber resilience using a combination of consulting, managed, cloud, and hybrid security services.

Managed Security Services

The threat landscape is evolving. Threats are becoming more frequent and sophisticated, and given the scale and frequency of attack, E&P companies are struggling to manage all aspects of cybersecurity in-house. Partnering with NTT Security as your Managed Security Services provider gives you access to our world-class specialist organization and security experts.

We're here to provide you with end-to-end 24/7 monitoring, management, and support of your security infrastructure. What really sets our Global Managed Security Services apart is our unique threat detection, advanced analytics, and unrivaled threat intelligence capabilities, and how we focus them on your industry. Wherever client relationships take your business, you'll have peace of mind and the convenience of being able to engage with one provider for all your cybersecurity needs.

Securing operational technology

In addition to conventional cybersecurity measures to protect information assets, operational technology (OT) security (OT) measures to protect production assets and ensure business continuity must also be considered as part of a continuous approach to cybersecurity and risk management.

Our team of OT experts will help you to design processes to improve your security profile with respect to IoT and SCADA systems. From technical services and access controls to encryption, design and assessment.

Our Advanced Security team continually conducts significant levels of research and development to find the best solutions for securing oil and gas industry operational technology.

Continuous compliance and consulting

The consequences of disruption to operations in cost, compliance and regulatory violations, and damaged customer confidence can't be ignored.

E&P companies still spend less than 0.2 percent of their revenues on cybersecurity, compared to three-times that proportion typically spent in the financial services sector.

– Bloomberg News

Creating, implementing and managing an up-to-date cybersecurity strategy is a significant challenge. That's where NTT Security comes in.

As consultants to energy organizations around the globe, NTT Security well understands the requirements of risk mitigation for upstream producers. Our proven methodology will significantly improve the security of your systems, protecting revenues and operational capabilities.

NTT Security experts will help shape each security process from a strategic and technical standpoint. This ensures that you are able to create a security infrastructure with the right security policies, processes, architecture, and expertise in place.

External advice can be invaluable to evolve a comprehensive security strategy and, using our proven Global Enterprise Methodology consultancy delivery approach, we will enable you to understand your risk exposure and make informed risk management decisions.

Cybersecurity issues in the energy sector

Underinvestment

On the back of extended low prices, oil companies in particular put investment in cybersecurity on hold in 2015 and 2016, while hackers grew increasingly sophisticated. E&P companies still spend less than 0.2 percent[1] of their revenues on cybersecurity, compared to three-times that proportion typically spent in the financial services sector.

Organized and specialized hacking threat

Attacks against oil and gas companies are growing in frequency. As many as 140 cybercriminal groups[2] are now targeting the energy industry, up from 87 in 2015.

State-sponsored actors

The former Deputy Director of GCHQ in the UK recently warned[3] the oil and gas industry to brace itself for the increased risk of cyber attacks from state-based hacking. With a complex ecosystem of computation, networking, and physical operational processes spread around the world, the industry has a large attack surface with many attack vectors.

High risk, high cost industry sector

The NTT Security Risk:Value 2018 Report[4] found that 61 percent of organizations in the oil and gas sector had suffered a security breach or expected to do so, compared to 55 percent across all sectors surveyed. The sector is also likely to experience a higher than average loss of income resulting from an information security breach. The financial impact on revenue reported by oil and gas organizations that took part in the Risk:Value 2018 research was 15.12 percent, compared to the average income loss across all sectors of 10.29 percent.

About NTT Security

NTT Security is the specialized security company and the center of excellence in security for NTT Group. With embedded security we enable NTT Group companies to deliver resilient business solutions for clients' digital transformation needs. NTT Security has 10 SOCs, seven R&D centers, over 1,500 security experts and handles hundreds of thousands of security incidents annually across six continents.

NTT Security ensures that resources are used effectively by delivering the right mix of Managed Security Services, Security Consulting Services and Security Technology for NTT Group companies – making best use of local resources and leveraging our global capabilities. NTT Security is part of the NTT Group (Nippon Telegraph and Telephone Corporation), one of the largest ICT companies in the world. Visit **nttsecurity.com** to learn more about NTT Security or visit **www.ntt.co.jp/index_e.html** to learn more about NTT Group.

1. Bloomberg News, April 2018: https://www.bloomberg.com/news/articles/2018-04-27/-cyber-blindspot-threatens-energy-companies-spending-too-little

2. Business Insider, May 2018 https://www.businessinsider.com/cybercriminals-are-exposing-oil-and-gas-but-the-industry-is-turning-a-blind-eye-2018-5?r=US&IR=T

3. The Independent, August 2018: https://www.independent.co.uk/news/uk/home-news/cyber-attacks-threat-oil-gas-industry-brian-lord-gchq-abu-dhabi-a8495666.html

4. NTT Security Risk:Value 2018 Report: https://www.nttsecurity.com/landing-pages/risk-value-2018