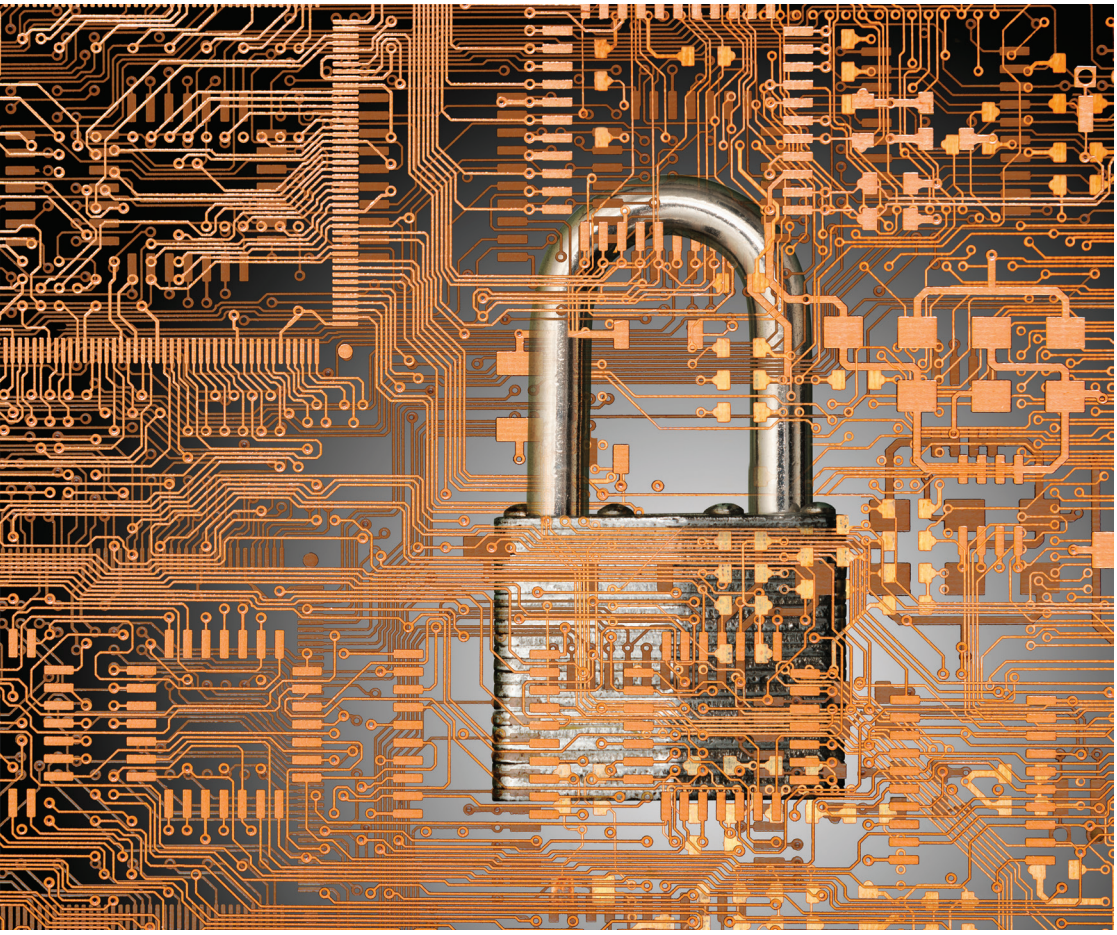
CYBER SECURITY



Oil and gas companies need an integrated 'security immune system' and a long-term strategic plan to protect their assets and IP from not only today's cyber threats, but also the inevitable more complex threats the future will bring

Photo: IBM

IBM's *Marcel Kisch*, *Amit Bhandari* and *David Haake* explain how the oil and gas sector can manage information and operational technology (IT and OT) security risks in a digital world.*

Internet of Threats

Cyber security in the oil and gas industry is a rapidly evolving, multi-dimensional challenge given the nature, scale, complexity and globalisation of the industry.

Firstly, oil and gas is a multi-trillion dollar, asset rich industry with millions of wells, thousands of miles of pipeline and hundreds of refineries. Oil and gas companies are among the largest enterprises in the world; strategic and multi-national in nature, they are served by a vast ecosystem of service providers. These characteristics make the industry and the companies vulnerable to security attacks for a variety of malicious intentions and consequences. The volume and sophistication of these attacks is on the rise (see **Figure 1**) and 'we don't know' becomes a less accepted response to a security incident. The risks extend beyond data breaches and financial losses, to worker safety, business continuity and 'right to operate' issues, regulatory compliance and reputational effects.

The latest example of such an attack was in December 2018, when a new Shamoon malware variant was discovered on the network of an Italian oil and gas contractor, where it destroyed files on about 10% of the company's servers – mainly in the Middle East, including Saudi Arabia, where the company conducts the vast majority of its business, although infections were also reported in India, Italy, and Scotland.

In addition, the nature of oil and gas business is changing as most companies are at some stage of their digital transformation journey. Even though digitalisation and automation is not a new concept for oil and gas companies (they have been working on digital oil fields, pipeline sensors, process control and automation in refineries for decades), the new digital evolution is blurring the traditional boundaries between corporate information technology (IT) and operational technology (OT). This convergence of operational and business systems increases the risk of a whole new array of cyber threats.

Finally, there are many new 'threat actors' in cyber security these days, including not just hackers, hacktivists and insiders using internet accessible freeware hacking tools, but well-funded nation states using the most sophisticated tools and techniques.

The bottom line is that managing IT and OT security can no longer be an after-thought for oil and gas companies in this digital era. The security transformation for the company should align and stay in-sync with the overall digital transformation agenda.

Investing beyond the barrel

In the digital era, to fuel their competitive edge and to accelerate their business transformation, oil and gas leaders need to invest beyond the barrels and towards protecting their other natural resource – data; especially operational data, assets and processes. They need to align with a strategic security partner to comprehensively predict, monitor, manage and respond to the

multi-dimensional cyber security threats.

However, the industry's primary focus, investment and success to date in cyber security has been on corporate data centre protection and fraud prevention.

The oil and gas industry is characterised by joint ventures and global operations, and this massive multi-national and joint asset base is vulnerable, more difficult to protect and often so critical (safety) that not every security control can be applied. Digital transformations linking oil and gas facilities and their markets through cloud-based ERP and Internet of Things (IoT) technologies are underway in the majority of oil and gas companies, but these initiatives often do not have a holistic or adequate security approach – especially with respect to OT such as SCADA networks and process control equipment.

The technological cyber defenses developed to protect enterprise IT can often only be transferred to the OT domain with some adaption. And as IT and OT get more interconnected, the security approach must be integrated to cover both IT and OT in a holistic threat picture, and OT related to cover specific real-time, reliability and uptime requirements that make some OT parameters unique.

Today, we are facing a security skills shortage in IT, but the security experts that understand operations are even more scarce. This situation will not be solved quickly. Looking across all industries, the move to greater automation and process networks is starting to gather pace.

The majority of oil and gas facilities are designed for full-time operations, making it more challenging to apply technical security controls (which in many cases have to be passive) to perform security assessments and roll-out patches. There is also a significant cultural and organisational gap between operations and IT security personnel, which work against the development of comprehensive and holistic security designs to prevent these downside risks.

A joint IT and OT approach is needed, which allows orchestration and alignment in prevention, detection, response and recovery. It increases transparency and improves enterprise performance, while offering gains in safety, reliability and security, as well as enabling IT-OT security governance.

You would think bridging the IT-OT gap would be something a company can do on its own, but often they struggle because the domains are so different, and the organisational units so far apart (Chief Operating Officer, COO; Chief Information Officer, CIO). This is often when small, specialised security companies come into the picture, because they can bridge the gap. However they also can fail when it comes to global service coverage or 24/7 security services for OT. The IT-OT security expert gap will not be closed anytime soon. Consequently, this is where augmented intelligence comes into play – better security insight, better risk awareness, quicker response and advanced security analytics and artificial intelligence (AI).

Risk awareness

Cyber-attacks in the OT environment can damage industrial facilities, and even result in fatal consequences. Oil fields, refineries, and gas processing facilities are dangerous environments, and when their control systems and networks are compromised, a crisis can quickly arise.

How can organisations react quickly and effectively to these growing IT and OT threats?

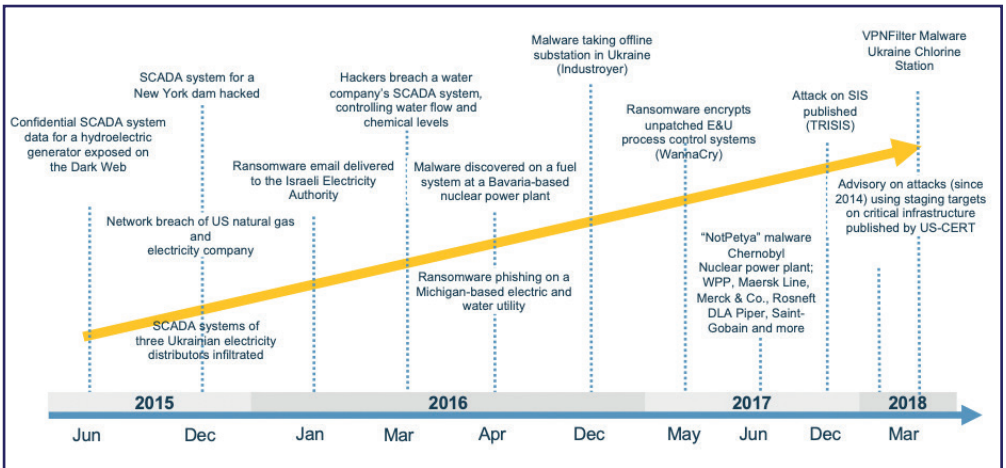


Figure 1: The volume and sophistication of cyber attacks on oil and gas facilities is on the rise
Source: IBM

Depending on the company priorities, one of the first steps is either to become risk aware for the OT environment, or identify gaps to existing industry/government regulatory compliance requirements. A quick risk review would include performing a passive penetration test on specific environments.

Once companies are risk aware, they can allocate budget and investment planning according to their risk management strategy. Monitoring of the OT network is one of the next steps, which allows risk insights and alerts in near real time and the monitoring can be extended to include endpoints, maybe even down to non-Internet Protocol based legacy equipment like sensors and actuators. All these point solutions can report into a central alerting system (SIEM).

In the later stages, if the company realises that they have too many incidents and need to improve their response capabilities, then IT-OT security operation centres (SOC) can provide major benefits.

Ultimately, these expansive, asset intensive, threatened global companies need an integrated 'security immune system' and a long-term strategic plan to protect their assets and intellectual property. Their security systems and specialists need to work seamlessly together to meet not only today's cyber threats, but also the inevitable more complex threats the future will bring.

With the oil and gas industry fast evolving, and the rate of digital transformation rapidly increasing, this IT-OT convergence is blurring the operational boundaries while giving rise to a potential 'Internet of Threats'. IBM believes that CIOs/CISOs need to present IT-OT security as a business issue at the senior leadership level consistent with a 'going-concern' business.

Cloud-based security monitoring, AI analysis, collaboration tools and access to regulatory authorities, security specialists and managed security providers are the industry's best vehicle for getting ahead of the threat actors. ●

**Marcel Kisch* is Global OT Security Business Development Manager, IBM; *Amit Bhandari* is North America Security Services Leader, Industrial Market, IBM; and *David Haake* is Director, Business Development, Chemicals & Petroleum Industries, IBM and an IBM Industry Academy Member.

For more information, see **https://www.ibm.com/security** and **https://www.ibm.com/industries/oil-gas**