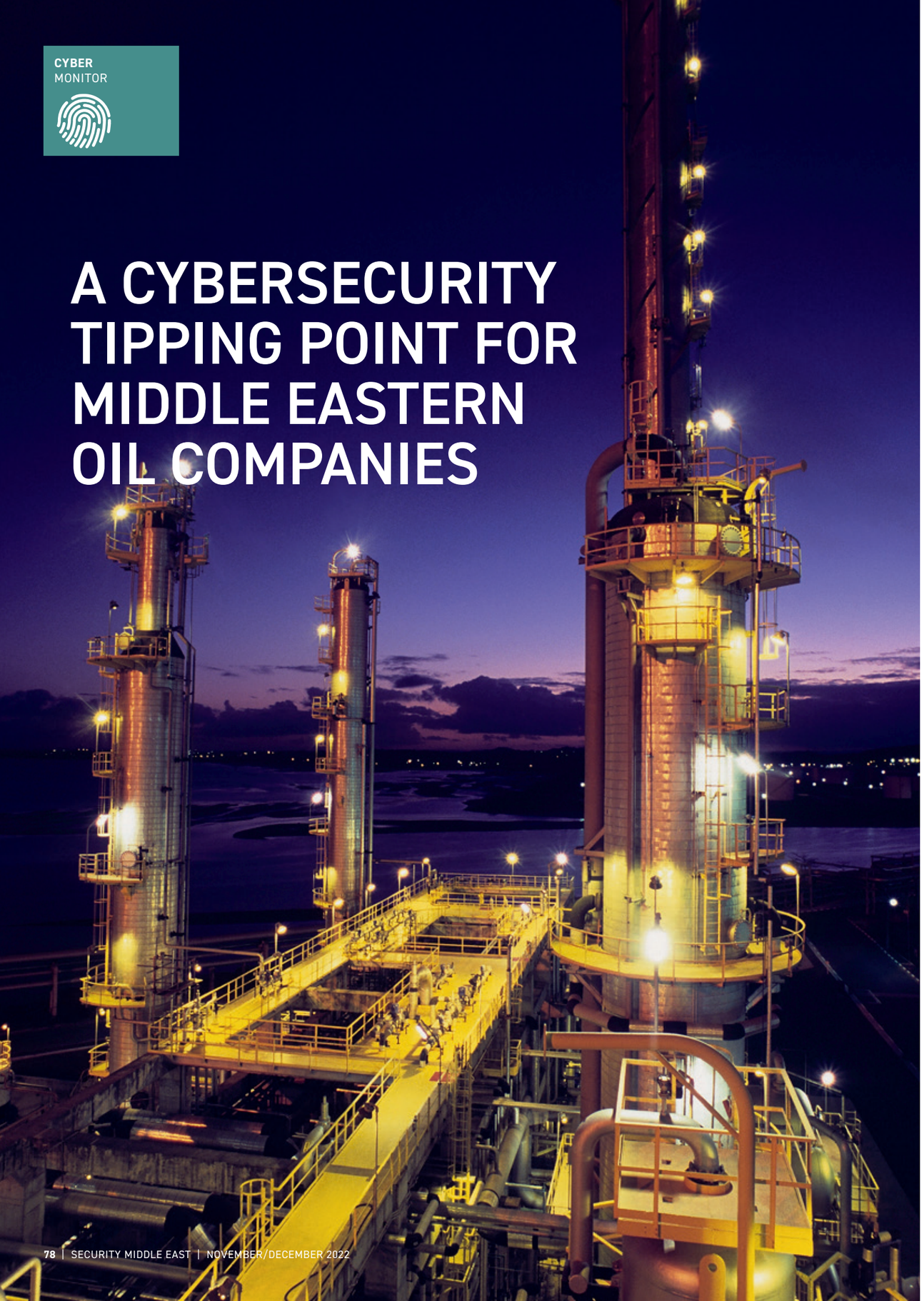
A CYBERSECURITY TIPPING POINT FOR MIDDLE EASTERN OIL COMPANIES



CYBER
MONITOR

More online connections means more opportunity for nefarious attacks exploiting gas and oil companies in the Middle East. **Glenn Braverman**, VP, International & Foreign Military Sales, Owl Cyber Defense, explains more

In 2012, one of the world's largest oil companies, Saudi Aramco, was the victim of a massive cyberattack that saw data wiped out from over 35,000 computers. The attack inserted the Shamoon virus into Aramco's network; Qatar's RasGas was hit a few weeks later. These events served as a wake-up call for the already security-conscious oil industry to further wall off operational technology programs to ensure continuity of operations.

Now, the oil and gas industry is at a similar turning point, albeit for different reasons. The growth of internet-connected devices and the efficiency gains from integrating them with existing operational technology provides an unavoidable opportunity to modernise.

However, the increase in online connections creates a larger surface area for cyberattacks. With nearly 40% of the oil industry concentrated in the Middle East, many of these companies find themselves as the target of state-sponsored and advanced attacks aimed at not just stealing data but shutting down operations.

Adversaries understand these locations' importance and their impact on the national and global economies. For example, in September 2019, two oil production facilities in Saudi Arabia were attacked by missiles that were shot from drones. Sadly, we see these types of incidents happening in highly volatile political environments.

Preparing for a new paradigm

As the industry moves forward, the cybersecurity boundary is much broader than it was a few years ago. The next phase of security for oil and gas companies will focus not just on protecting network boundaries but also interconnections between devices.

The need for this security comes during a contentious time. The war in Ukraine has helped fuel a global energy crisis, raising gasoline prices to their highest mark ever in many parts of the world. Even before the crisis, Middle Eastern oil companies were already exploring new oil deposits and liquefied natural gas at a historic rate. New explorations and facilities create additional operational theatres that are costly to staff, maintain and protect. In the absence of localised cyber defenses, oil companies may use remote monitoring systems that leverage interconnected devices to operate and enhance the cybersecurity footprint. But those connected systems increase the attack surface. Given this dramatically changing landscape, a different approach to cyber protection is needed.

The future of cyber for the oil industry

This past May, oil companies made a collective pledge at the World Economic Forum to reinforce cyber resilience against dangerous attacks and to "modernise global commitment" across industries. "As the world deepens its digital footprint, cyber threats are becoming more sophisticated," said Amin H. Nasser, CEO of Saudi Aramco. "But one company, working alone, is effectively like locking the front gate while leaving the back door wide open."

These companies operate as competitors, but understand the collective need for enhanced cybersecurity. The belief is that an attack on their part of the infrastructure could create a cascading effect that impacts all of them.

Now the hard work must genuinely begin. Oil companies should utilise a full bi-directional approach that allows for the ability to monitor and pull sensor log data into a centralised view across the enterprise. Investing in cross-domain visibility solutions will provide an integrated approach to monitoring software and hardware that can ensure segmentation of sensitive data traversing throughout the Middle East and other global locations, significantly lowering the risk of cyberattacks.

Other considerations include:

- The ability to leverage software development for unique protocols.
- Specific hardware that can separate the networks through either electrical or optical isolation.
- An understanding of every piece of data that is in use, whether it comes from database replications, a Syslog, or files transferred between locations.

The path forward

While the oil and gas industry has long led cybersecurity for critical infrastructure, in light of recent events, the criticality of the resources they produce mandates their continued pushing of the cyber envelope. The moves the industry makes today will serve as a template for other critical infrastructure stakeholders.

The oil industry is on the precipice of a new era. The increased use of interconnected devices has already revolutionised how these companies operate. The true growth and potential of digital assets in the connected device era can only truly be realised when the data they collect and transmit is secure.

www.owlcyberdefense.com