PHOTO SHUTTERSTOCK

COUNTERING THE HACKER THREAT

A systematic approach to cyber security can help to avoid costly attacks on critical oil and gas installations

Cyber attacks are growing in scale and complexity, becoming more difficult to detect and defend against, and costing companies increasing sums of money to recover from.

The energy and utilities industry, including oil and gas, suffers average annualized losses from cyber crime of USD13.2 million per sampled organization, according to a 2014 survey for Hewlett-Packard.[1] This figure, 24% higher than the 2013 findings, represents the highest for all industries included in the IT company's research. One incident by unknown hackers in 2014 affected around 300 energy companies in Norway, the country's biggest such attack.[2]

Upstream oil and gas responds

"Consensus exists that cyber attacks are growing more significant and serious," said Paul Reither, vice chair of the Security Committee of the International Association of Oil & Gas Producers (IOGP), the voice of the global upstream industry. "Furthermore, attacks against computer systems can produce a physical outcome that cannot be ignored."

IOGP defines three key threats: theft of core intellectual property; disruption or destruction of a physical plant and other points of capital investment; and compromise of executives' communications about key business decisions. "Within this context, cyber is now part of a holistic approach to security for the industry," Reither commented.

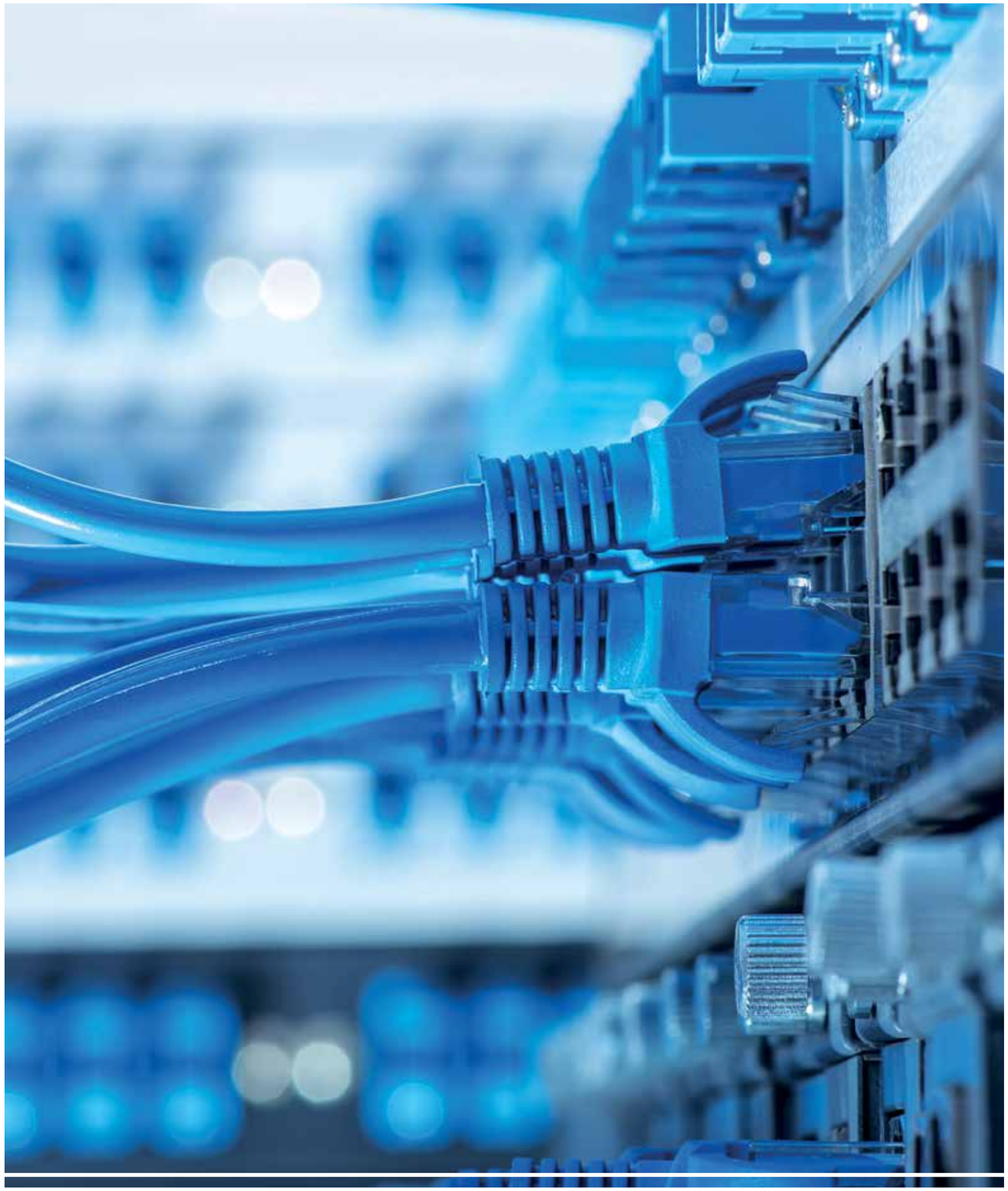
> "Consensus exists that cyber attacks are growing more significant and serious"
>
> Paul Reither, vice chair, Security Committee, International Association of Oil & Gas Producers

Direct threats can, he explained, be either heterogeneous or advanced persistent threats; a combination of malware and hacker tools; or attacks from organized crime, rogue states and/or terrorist groups.

"Tactics can include 'social enginering', psychological online manipulation to trigger damaging actions or obtain confidential information," he added. "Cyber is not a threat in itself, but an increasingly effective means to carry out threats."

Principles developed in international standards such as ISO, IEC or NIST should be sufficient to tackle overall IT security risks and protect against homogenous IT/cyber threats not specific to the upstream industry, Reither suggested. "However, IOGP will support efforts to improve standards coordination and learning," he added. "Member companies should develop mitigation based on risk assessment, and adopt international standards in line with the level of threat."

IOGP sees a "very low" probability of a massive cyber attack disabling production, refining or distribution infrastructure. "It is very difficult to attack complete infrastructure by the means through which Shamoon malware hit Saudi Aramco in 2012,"[3] Reither commented. "That compromised many homogenous computer systems designed to run a fairly broad set of >



1 '2014 Global report on the cost of cyber crime', Ponemon Institute research for HP Enterprise Security, October 2014
2 '300 oil companies hacked in Norway', thelocal.no, 27 August 2014
3 'Exclusive: insiders suspected in Saudi cyber attack', Reuters, 7 September 2012

CYBER SECURITY

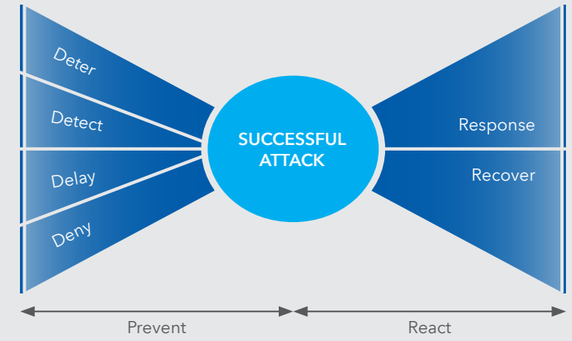
Interconnected IT infrastructures and technologies have modernized management of oil and gas operations, but increase the risk exposure of critical cyber structures

Figure 1: The Top 10 digital vulnerabilities of the Norwegian oil and gas industry

1. Lack of cyber security awareness and training among employees
2. Remote work during operations and maintenance
3. Using standard IT products with known vulnerabilities in the production environment
4. A limited cyber security culture among vendors, suppliers and contractors
5. Insufficient separation of data networks
6. The use of mobile devices and storage units including smartphones
7. Data networks between onshore and offshore facilities
8. Insufficient physical security of data rooms, cabinets etc
9. Vulnerable software
10. Outdated and ageing control systems in facilities

Source: DNV GL assessment for Norwegian ministry of justice and public security, April 2015

Figure 2: Cyber security version of bow-tie model used in managing safety risks



Source: DNV GL

Cyber security vulnerabilities (Figure 1) can be addressed through a risk based approach based on the bow-tie model familiar in barrier management (Figure 2)

applications. Luckily, it did not cross over to computers involved in the production of oil and gas."

It is, however, suspected that hackers injected malicious software into the control network of the Baku-Tbilisi-Ceyhan pipeline, Turkey, in 2008, causing a huge explosion.[4]

Connectivity raises risk

Headline incidents are rare, but many lesser attacks go undetected or unreported. "Many organizations do not know that someone has broken into their systems," said Pål Børre Kristoffersen, principal consultant, DNV GL – Oil & Gas. "The first line of attack is often an office, business or enterprise IT environment, which could help hackers to access more critical production networks, process control and safety systems."

While office IT is segregated from industrial systems, separation mechanisms between a company's internal networks are often weaker than against external networks, he explained.

Hackers may also use social engineering attempts on office domains to harvest passwords and other ways to access production networks.

Increased exposure of critical systems to external networks is a key reason for heightened digital vulnerability, according to DNV GL's analysis of Norway's maritime and oil and gas sectors (figure 1, page 21).

This reflects trends towards remote operation and maintenance, and management systems that transport large volumes of process data to the office domain. Due to limited fibre capacity and redundancy, networks are shared, introducing vulnerabilities. Supplying offshore power from onshore facilities introduces risk as electricity grids are digitally vulnerable.

> "Supervisory control and data acquisition software and other control systems are main targets"
>
> Tor-Erik Hansen, technical manager, Martin Linge project, Total E&P Norge

DNV GL found that few Norwegian maritime and offshore oil and gas organizations use systematic approaches to preventing, detecting and protecting against cyber security challenges, whether sophisticated attacks or accidental breaches.

"Operators perhaps tend to think that cyber security is for technical devices and that firewall protection, virus security and passwords suffice; but eliminating cyber risks requires a defence-in-depth strategy beyond basic measures," Kristoffersen said.

"Countermeasures can be established using a barrier management approach familiar from managing health, safety and environment risks (page 21). Cyber security requires the same vigour as barrier management of HSE risks."

Case study: Martin Linge

DNV GL is assisting Total E&P Norge with cyber security risk management for the Martin Linge field development and associated operations offshore Norway. DNV GL's scope of work includes day-to-day coordination of cyber security during preparations for operation, with a specific focus on integrated control and safety systems. The initiative also aims to raise awareness of cyber security risks and to train personnel to take simple preventative measures.

"DNV GL's experience has been a key contributor to identifying and defining cyber security risk," said Tor-Erik Hansen, technical manager for the Martin Linge project, Total E&P Norge.

"Supervisory control and data acquisition software and other control systems are main targets. These normally originate externally from the business network, so it is equally important to prevent and stop attacks through this route."

Internal attacks by malware planted in vendor-supplied software are another important risk that requires procedures for checking all such software, he added.

Total's approach is to assure compliance with company rules for IT system architecture and firewall implementation. Links between industrial and business networks are avoided if possible. A systematic approach is taken to implementing and monitoring the effect of cyber security barriers. For Martin Linge, remote access will be allowed only from the onshore operation centre, where access to the hub management interface is strictly controlled.

"We feel we are a front-runner in Norway, and maybe worldwide, in having an onshore control room from day one of this project's operation," Hansen said. "We have taken a large technological step in pulling all networks to shore for Martin Linge. This creates risks. However, we believe that, on completion, we will have established a way of working that could guide others."

Total E&P Norge has strong links to Total headquarters in Paris for business and industrial cyber security issues. The cyber security team in France has contacts in all other major oil companies so that information and alerts can be shared rapidly.

Separate personnel are responsible for cyber security of the industrial and business domains at Total E&P Norge, and for maintaining direct communication with their counterparts. "We also intend to set up systems to receive alerts from Norwegian cyber security authorities as rapidly as possible," Hansen said.

He expects that it will become a default position for relevant authorities worldwide to insist that, like Total, the oil and gas industry handles cyber security issues seriously and systematically. ■

SECURITY BARRIERS

By using a bow-tie model for security barrier management (figure 2), companies can identify threats to operations, and plan barriers to prevent incidents and mitigate consequences. This includes procedures to maintain barrier quality documented in performance standards.

Bow-ties and performance standards for security management are just two tools that DNV GL applies in its independent, risk-based approach to designing, implementing, testing and maintaining cyber security countermeasures for customers worldwide. The company's software tool, Synergi Life – Risk Management Module, is used to establish a live asset and risk registry. The tool enables the assessment of vulnerabilities and threats, as well as mitigation follow-up.

DNV GL's approach is founded on broad industry expertise and experience in implementing relevant national and international security standards, best practices and tools. It is also investing in initiatives to develop pan-industry best practice in identifying, preventing and responding to cyber security threats.

4 'Mysterious '08 Turkey pipeline blast opened new cyberwar', Bloomberg, 10 December 2014