CYBER SECURITY

Tackling the cyber attack pandemic

Cyber attacks are a growing risk in the oil and gas sector with the move towards digitalisation in the energy transition. Fortunately, new solutions are being developed to address the IT and OT threats. *Brian Davis* reports.

Digitalisation of the energy sector is a two-edged sword – optimising the business and global operations while also facing a growing threat of cyber attack in a highly connected network of physical and digital assets.

The Internet of Things (IoT) opens new opportunities as digitally connected physical assets with operational technology (OT) and advanced information technology (IT) improve efficiency, enhance safety and optimise operations with innovative apps, big data analytics, sensors and artificial intelligence (AI). However, industrial IoT can have significant vulnerability in terms of cyber security, and critical infrastructure can be hijacked or destroyed by criminal enterprises.

A highly publicised attack earlier this year demonstrates the scale and cost of failure to monitor, detect or act on potential cyber threats.

In April 2021, hackers took down the Colonial Pipeline, the largest pipeline in the US, as a result of a compromised password. Hackers gained entry through a virtual private network (VPN) using a password that was leaked on the Dark Web. A week later, an operator in Colonial's control room received a ransom note demanding a large sum of cryptocurrency in exchange for a new password. The company, which transports 2.5mn b/d of fuel, immediately shut-down operations and reputedly paid $4.4mn to a Russia-linked cyber-crime group known as DarkSide.

In December 2017, a Saudi Arabian petrochemical plant reported a malware attack, since known as Triton or HatMan, that went far beyond other industrial attacks (like Stuxnet) by directly interacting with an automated safety instrumented system (SIS). Worryingly, these are considered to be the last line of safety defence for industrial facilities, designed to prevent equipment failure and catastrophic incidents such as fire or explosions.

Industrial cyber security company Nozomi Networks set out to learn how the Triconex controller from Schneider Electric, used at the facility, could become the target of attack by a malicious code. By reverse engineering the TriStation software on the engineering workstation that communicates with the SIS controller, Nozomi Networks was able to develop two tools to allow an engineer to view communications with the controller and detect Triton malware activity in network communications.

Nozomi Networks also offers an AI-based solution that runs on the cloud to identify OT vulnerabilities that have to be fixed upstream and downstream, to mitigate risk without blocking day-to-day production.

A growing threat

According to a recent SANS Institute OT/ICS cyber security report (August 2021), industrial control system (ICS) cyber security threats are growing in severity. About 48% of organisations surveyed don't know whether they have been compromised. 'It's deeply concerning that nearly half of this year's survey don't know whether they have been attacked when visibility and detection solutions are readily available,' remarks Nozomi Networks Co-founder and CEO Andrea Carcano.

About 70% of the ICS survey respondents rated the risk to the OT environment as 'high or severe'. Ransomware topped the list of threat vectors (54%), while unprotected devices were cited as a risk by a third of respondents. Of the 15% of respondents that had experienced a breach in the last 12 months, 18% said the engineering workstation was an initial infection vector. Generally, external connections were seen as the main point of access for cyber attacks (49%) with remote access services seen as vulnerable by 36%.

'Connectivity to external systems is a root cause of incidents, and an indication that many organisations fail to follow network segmentations best practices,' says Mark Bristow, the report's author. On the plus side, the SANS report notes an 'overall increase' in budget allocation for ICS cyber security.

OT cyber security practitioners are advised to keep threats and perceived risks at front of mind in the face of a growing risk environment. However, incidents often go unreported because of corporate sensitivity. And despite the threat, monitoring and detection ranked 'relatively low' among survey respondents, with only 12.5% confident that they had not experienced a compromise in the last year.

'You can't protect what you don't see,' notes Carcano.

Aker BP onshore operations centre
Photo: Aker BP

'Historically, cyber security was not considered important in the original industrial control system design but has become necessary as systems have evolved.'

Andrea Carcano, Co-founder and CEO, Nozomi Networks

It is vital to have visibility of critical control components, like pumps, compressors and centrifuges. Historically, metering components such as programmable logic controllers (PLCs) are analogue on one side, connected to a pump or temperature gauge, for example, but digitally connected on the other side. 'Historically, cyber security was not considered important in the original industrial control system design but has become necessary as systems have evolved,' Carcano says.

Basically, you need to have a clear picture of all the components – which is easier said than done in global energy operations. Several years ago, most energy companies struggled with this component visibility issue. 'You need a different type of digitalisation for plant cyber protection,' he suggests. Nozomi Network's solutions are designed to interact with any device, supporting over 150 protocols and providing full visibility of different components as they communicate with each other.

'You have to understand clearly where you are vulnerable', says Carcano. 'The main challenge is to have visibility of a plant designed 10–20 years ago, operating 24/7. The next step is remediation, which means finding a window of opportunity, which is sometimes months away. Furthermore, cyber security must avoid disruption of day-to-day operations. The loss of an occasional email is manageable in IT systems, but you need to think differently at the plant level.'

'The future is here already – with IoT, edge computers and sensors talking on 5G – but I'm not sure if the industry is ready for all those components from a security perspective.'

Sigmund Kristiansen, Chief Information Security Officer, Aker BP

A robust approach

Industrial cyber security is the oil and gas industry's Achilles heel. Attacks on the oil and gas sector have increased exponentially. Given the move towards digitalisation, the big challenge is to bring old systems online, as they are rarely maintained or patched sufficiently and lack visibility. The gap between defenders and hackers is increasing.

Strong cyber security requires a collaborative approach. In the oil and gas sector, supply chains are interconnected and interdependent, so cyber security should be addressed end-to-end. Indeed, the same tools that help oil and gas infrastructure run efficiently and support remote operation are potential points of exposure for cyber attacks. Where past attacks focused on IT, attacks on OT are now more common.

Building robust cyber security can be a challenge. The World Economic Forum (WEF) white paper on *Cyber resilience in the oil and gas industry*, offers a playbook for boards and corporate officers, as a blueprint for companies to secure critical infrastructure and address cyber risk. The WEF working group offers six principles to help boards at oil and gas companies strengthen cyber resilience:

- *Cyber security governance* – should have broad participation in an organisation, aligning efforts with clear accountability.
- *Resilience by design* – with cyber security as a design parameter of corporate culture.
- *Corporate responsibility* – recognising that complex, frequent attacks mean organisations should examine cyber risks and take responsibility for managing them.
- *Holistic risk management approach* – as cyber risks require a mandate, resources and accountability to mitigate risks in all parts of the value chain, so one weak link doesn't bring production to a halt.
- *Ecosystem-wide collaboration* – as weak links may lie outside an organisation, best practices must improve cyber security across the whole sector.
- *Ecosystem-wide cyber resilience plans* – to help mitigate damage from attacks that succeed.

A risk-based approach

Aker BP operates five assets on the Norwegian Continental Shelf, including Valhall, Alvheim, Ivar Aasen, Skarv and Ula, and is partner in a number of other licences. Sigmund Kristiansen, Chief Information Security Officer (CISO) at the company, heads the cyber security and risk department, with responsibility for the operation and governance of cyber security in Aker BP.

He recognises there are different challenges securing IT and OT. 'However, they are becoming more connected as IT and OT merge,' he notes. The other security dimension is brownfield versus greenfield. 'Brownfield operations have a lot of "technological debt" that raises security risk, because old tech doesn't support modern security methods but relies on old, vulnerable protocols that can be exploited by hackers or threat actors – as seen by the damage caused to the Ukrainian energy system and the Colonial Pipeline malware attacks.'

Older OT systems tend to be static. Updates are rare, costly and time consuming, as the whole environment around a component needs to be tested for risk. Whereas IT and cloud solutions are updated regularly.

The cyber security manager should look at total risk, as networks have different access rights for different users according to the environment. 'I'm concerned about total risk,' remarks Kristiansen. 'There is also an operational risk. If you start changing a system, the behaviour changes. The ultimate goal is to have a stable, safe and reliable platform, vessel or subsea installation.'

Aker BP uses the industry standards for networks and access regimes, in accordance with Norwegian oil and gas recommendations based on ISO27000 series and IEC62443 for offshore operations, and NIST (US National Institute of Standards and Technology) standards for onshore operations, as a baseline. The organisation has a detailed security programme covering daily routines, periodic maintenance and a risk-based approach.

Governance documents have been developed, covering the management and security of different technologies. 'Some are prescriptive (ie like the number of characters in a password) and some are generic (eg where a firewall is required),' Kristiansen says.

However, he is cautious about cloud operations. 'As a minimum there should be some industrial standards. The future is here already – with IoT, edge computers and sensors talking on 5G – but I'm not sure if the industry is ready for all those components from a security perspective. Also, as offshore operations are increasingly controlled from onshore, cloud solutions will require a different security model.'

He agrees with the WEF recommendations. 'You need to have ownership of the cyber risk at board level, with a clear mandate to the CISO role, and a requirement that cyber security is integrated with the core business processes – reporting back metrics of the cyber risk.'

Kristiansen recommends: 'Cyber security should be treated as a business process rather than a technology process, since safeguarding a company's people and valuables is the No.1 priority.' ●