**The scale of cyber-attacks has grown with the proliferation of connected systems and devices that share data in energy networks. Malware, like the infamous Stuxnet, have been designed to target physical assets through industrial control systems. Since last December, cyber-hackers managed to take control of the electricity grid in a multi-pronged attack on Ukraine; others targeted a dam in the US, and hackers have disrupted interstate pipelines distributing oil or gas through long-haul networks. Over the last 12 months, nation state actors have been testing their cyber warfare capability both in the US and abroad. There have also been less publicised attacks with malware that continue to persist with large oil and gas companies on a consistent basis. Digitally enabled distribution networks and electric grids are critical to improving energy efficiency; however, they also raise physical security and cybersecurity concerns. In a recent survey by Accenture Technology Vision, more than half of utility executives reported that their organisation had suffered from twice as many privacy or security breaches compared to two years ago. Jim Guinn II, Global Managing Director of Accenture Resources – Cybersecurity, emphasises the importance of energy businesses investing in robust security solutions to support their digital transformation strategies. He suggests hackers should be kept at bay on two fronts. First, there is the continued risk to information technology (IT) systems that support a company’s enterprise functions. Second, there’s the risk to operational technology (OT) assets and industrial control systems. Furthermore, the growing IT-OT convergence means these threats are becoming one and the same. ’Industrial control systems were designed with uptime between failure to be number one priority,’ says Guinn. ’The control systems are typically highly resilient technologies that have been in the field for decades or more, they are in refineries, plants, multi-jurisdictional pipelines or oil and gas platforms. However, cybersecurity was not as significant an issue when many of these systems were deployed, so security was not at the forefront of design.’ He continues: ’Short of doing a complete workover or turnaround on these assets, a lot of these vulnerabilities are going to continue to persist until these systems are replaced by technologies with tighter cybersecurity controls.’ The challenge is how to isolate these systems, monitor and analyse performance. So if there is a vulnerability or breach, the operator can be aware and take action before catastrophe occurs and they experience loss of data, IP or brand damage. Guinn maintains: ’It’s more about management of these assets and understanding your risk profile than complete replacement, because the cost of replacement is significantly higher in many cases than the risk of a breach.’

**History of attack**

An Accenture position paper on cybersecurity noted a history of cyber-attacks from Night Dragon and Stuxnet to various malware attacks on energy, oil and gas majors and utilities. Guinn notes: ’There has been an increase in cyber-attacks within the energy continuum that are growing 20–45% annually, according to ICS, US-CERT and UK national grid reports. Let alone those cyber-attacks which are not reported because of commercial sensitivity.’ In his opinion, there is great cause for concern at senior executive level in major oil and gas companies and integrated pipeline distribution companies, about how to implement effort and direct financial and physical resources to rectify potential cyber vulnerabilities. Guinn suggests two issues should be addressed: ’First, you have to plan for cyber-attack. Sharing information is vital in order to be able to respond and recover. As with the safety briefing in a refinery which every refinery employee has to undergo, the same should happen from a cyber perspective.’ Second, analytics should be applied to industrial control system (ICS) networks to monitor abnormal behaviour and thwart cyber-attacks are on the increase and the Internet of Things (IoT) opens the oil and gas business to a new level of vulnerability. Though there is no silver bullet, improved security is doable, reports Brian Davis.
Major security improvement initiative

Accenture is currently working with one of the world’s largest oil and gas companies in a major transition from its legacy security platform to an industry-leading approach that includes the latest cyber, physical and industrial security systems.

The company needed to improve security from practically every angle. Recognising that preventable human errors cause nearly a third of all information incidents, the oil and gas major sought to underpin the entire security approach with an often overlooked, but critically important component, by heightening its employees’ awareness of how their day-to-day actions impact security.

As part of the solution, Accenture developed an extensive change-management programme to improve its employees understanding of security and behaviours. The consultancy began by collecting data on employees’ typical information security-related behaviors (eg frequency of changing passwords, attitudes towards risks, awareness of code-scanning services and many other tangible measurements). Accenture then identified 10 specific high-risk issues and helped set measurable objectives for the programme and established processes to regularly monitor progress.

In particular, the team created materials to help the employees recognise the threat from phishing email. Simulated phishing messages were sent to every employee. Anytime a recipient incorrectly clicked on a link in a simulated phishing message, that person immediately received additional information about phishing threats and how to take the correct action. Accenture’s security education programmes included interactive online games, instructional videos, a new website, exhibition booths during the client’s annual Safety Day, flyers, infographics and IT health checks.

attacks in real-time. ‘Because ICS are probably the most predictable networks from an analytics perspective and are much easier to monitor than an IT environment,’ he reflects.

Industrial Internet of Things

The broad acronym for sensing devices in the process control arena is IIoT, the Internet of Things, which when thoroughly integrated can lead to highly efficient oil and gas production operations. Nevertheless, networked devices can open the door for cyber-attacks. Automation, SCADA and IIoT devices allow oil and gas companies to optimise and remote control equipment for improved production performance. However, Accenture advises that systems need to be protected end-to-end with encrypted devices and networks so plant, pipelines and wells cannot be hacked.

The Industrial Control Systems Cyber Emergency Response Team reported 245 attacks in the US against control systems from October 2013 to September 2014, with the highest percentage (32%) on systems governing energy production and distribution.1

Guinn explains that IIoT is much broader than just ICS and includes SCADA, process and decision control as well. IIoT via IP [Internet Protocol] connects devices for operational control allowing business decision-making across a host of technologies. It’s not just a remote terminal unit (RTU) that sits on a pipeline giving pressure and volumetric readings. IIoT and IIOT also deal with the remote workforce using devices or tablets that can read sensors and detect operational patterns.

Admittedly there is no silver bullet. ‘I suggest that energy companies understand their cyber risk profile and focus on what they are most worried about – their most critical assets,’ says Guinn. ‘Once you have done that, you need to look at the threat actors to see what your likelihood would be as their target. Then you can build a more focused cybersecurity strategy to protect those assets.’

This may mean preventing people from taking devices into data centres, for example; blocking outward communications from human machine interfaces (HMI); and limiting other external communications and connectivity. At least one global oil and gas company forbids any connectivity of their process control environment with the outside world, whether using a USB, smartphone or disc. The company was driven in this direction by fear of a breach, when Indicators of Compromise (IoC) on their process control network led them to take this drastic step.

According to government sources, the two biggest threats of cyber-attack come from insider threats (which could include someone losing a PC with critical information on it) and phishing attacks by nation state actors. Fuel retailers also face organised crime trying to steal credit card information. ‘Ultimately, the most effective way to address this threat is education’, remarks Guinn. This means having a continuous security education programme within the organisation.

Being safe and sound means being aware of the threats. As mentioned, a recent Accenture Strategy survey revealed that 63% of energy executives said their organisations experience significant attacks on a daily or weekly basis.

Fortunately, there are simple ways that oil and gas companies can make big improvements in industrial cybersecurity. A good way to start is investing in general cybersecurity education for employees. It also helps to select a recognised industry standard/framework for cybersecurity, like the National Institute of Standards and Technology (NIST) cybersecurity framework in the US, so companies can measure and assess themselves, test resiliency and implement strategies for defence and recovery based on this cybersecurity framework.

Finally, a company should align its enterprise IT and OT organisations. But this is often easier said than done. Guinn warns: ‘Without executive alignment of both teams, many industrial cybersecurity programmes are set to fail.’

1 ICS-CERT Monitor Sept 2014–Feb 2015

How to be safe and secure from cyber-attack

So how can oil and gas organisations operate in a more safe and secure way? Accenture advises:

- Start with a big picture of how security efforts support business performance, balancing the cost of security with the impact it may have on your business.
- Establish effective communication channels and relationships with IT, the operations business (OT) and outside service providers.
- Clearly define roles and responsibilities for teams that manage cyber defence and incident response, including how they need to work together in the case of a breach.
- Conduct robust security operations monitoring threat intelligence, technical intelligence and vulnerability management as an integrated continuous process.
- Enhance and train incident response and recovery teams.

Petroleum Review | October 2016 19