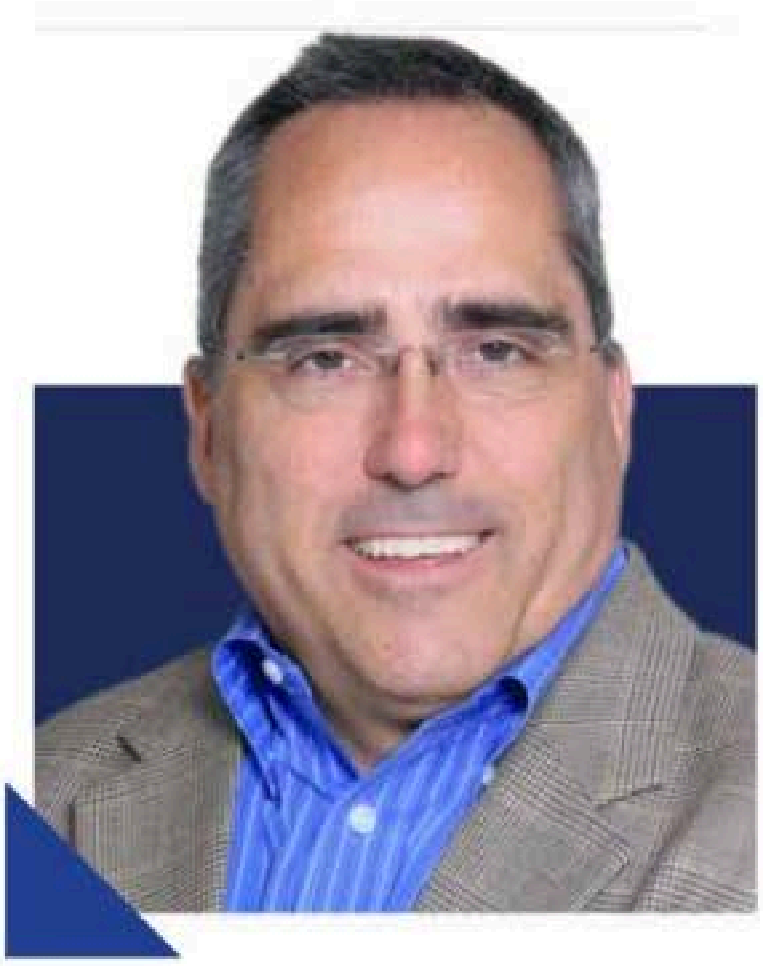
FUELLING THE FUTURE OF SECURITY



DENNIS LANAHAN, DIRECTOR OF WORLDWIDE CHANNEL PARTNERSHIPS & INTERNATIONAL SALES, OWL CYBER DEFENSE, DISCUSSES THE TRENDS SHAPING CYBERSECURITY IN THE OIL AND GAS COMPANIES.

What does digital transformation really mean for the oil and gas industry?

Digital transformation is all about improvement through data. The more you know about the past, present, and potential future operation of your systems, the more efficient, productive, and safe you can make them, and the better you can predict what might happen next. For the oil and gas industry, that means higher outputs, less downtime, and complete visibility into all aspects of the upstream, midstream, and downstream processes. However, with increased visibility and access comes the potential for cyber-attacks and interruption of service which is why companies are investing so heavily in cyber protection.

What are some of the opportunities for oil and gas companies around new technologies such as blockchain, AI and IoT?

As operational data becomes more abundant and available, predictive analytics allow oil and gas companies to predict when their devices and equipment might break down, diagnose abnormal behaviors, and find new opportunities for growth. AI and the IoT (and IIoT) are bringing these types of insights to the next level, with machine learning and advanced modeling that can be done faster and easier than ever before. It sounds cheesy, but computers really can help oil and gas companies "see into the future" and stay at the forefront of their industry.

What are the main challenges in implementing the digital oilfield concept?

Updating equipment can be challenging without introducing costly downtime and change management. Standardising software and protocols can also be painful, especially when supplanting an existing or aging infrastructure. One of the biggest challenges that comes up over and over is cybersecurity. From lack of integration expertise to lack of security personnel, not to mention the huge range of equipment, devices, and infrastructure involved across the entire industry, it can be a massive hurdle to overcome for an industry that is just now getting to where many other industries have been for a while in terms of digital maturation.

What are the top cybersecurity risks in the oil and gas industry, and what are your tips for overcome them?

Most OEMs still don't build cybersecurity into their products, so unless every piece of connected equipment and firewall is constantly patched and monitored, it can be an exhausting, frustrating task trying to keep everything secured. That's why you're seeing a lot of operators move to less time and effort-intensive security, like data diodes, that they can basically set and forget as they continue to grow their digitised operations. There's substantially less risk in a hardware-enforced device than a software-based security system, because it basically trusts nothing outside the secured perimeter – even cyber insurance costs can be lowered in some cases.

How different is OT security from that of IT security?

Today, the primary difference is what needs to be protected. For OT it is the equipment and operations, for IT it is data. Financial data, personal data, and PHI are far easier to exploit for monetary gain and is what IT security focuses on. In the OT space attackers are looking to cause harm to the systems themselves, not steal data, so the focus tends to be more on securing the network than the data itself. OT also tends to have more of an emphasis on efficiency and safety rather than security and confidentiality. This means that there are almost always less cyber security personnel to help improve and oversee the security of OT systems. However, over time the difference between OT and IT may become more semantic, as they become increasingly entangled and as OT catches up to the sophistication of IT.