The digital revolution is creating immense opportunities for oil and gas companies who harness the power of IoT and data-driven solutions. However, to safely capitalize on the efficiencies and benefits afforded by increased connectivity, organizations must be prepared to respond to an evolving security landscape in which cyber threats are the new norm.

Offshore facilities present an especially attractive target due to their perceived vulnerability and the catastrophic damage that can arise from a successful attack. In light of this, offshore operators can no longer delay protecting their operational technology (OT) assets. They must come together with partners and government to bridge the cyber readiness gap and realize the full potential of digitalization.

Two types of companies exist in the oil and gas industry today: those who have been attacked and are aware of it, and those who have been attacked and are not aware of it. In recent years, an increasing number of these attacks have been directed at OT (i.e., the machines, systems, and networks that make up physical infrastructures and digital inputs). In addition to being older than IT systems, and often less protected, an interconnected network of physical assets provides a larger attack surface that is difficult to secure. Cyber attackers are realizing the wide-ranging impacts that penetrating OT infrastructure can have – from stealing, disrupting, and destroying data, to directly affecting critical operations and safety.

Attacks against OT have risen from 5% to 30% in a few short years and range from disrupting SCADA and industrial control systems, causing outages and safety issues, to ransomware attacks, where systems are held hostage with threats to disrupt and destroy operating systems. The primary challenge industries like oil and gas now face is how they can secure a complex, open ecosystem without impacting performance.

With the chance of being attacked in today's environment now 100%, the offshore industry can no longer wait to address cyber vulnerabilities. Unfortunately, far too many companies still believe that the easiest way to protect their operations is by “air gapping” (i.e., physically isolating offshore infrastructure from potentially unsecure networks). But this misguided approach will not make them safer. In fact, greater connectivity equals insight. Visibility enables organizations to recognize abnormalities and react when a cyber attack does occur.

Moreover, air gapping does not protect against inside threats, which often pose the greatest risk to critical operations. In a recent survey of 377 oil and gas security professionals, 65% of respondents said that a negligent or careless insider was their top cybersecurity concern, while 15% said it was a malicious or criminal insider. Overall, 59% of respondents said that OT is now a greater concern than IT.

With the chance of being attacked in today's environment now 100%, the offshore industry can no longer wait to address cyber vulnerabilities. Unfortunately, far too many companies still believe that the easiest way to protect their operations is by “air gapping” (i.e., physically isolating offshore infrastructure from potentially unsecure networks). But this misguided approach will not make them safer. In fact, greater connectivity equals insight. Visibility enables organizations to recognize abnormalities and react when a cyber attack does occur.

Moreover, air gapping does not protect against inside threats, which often pose the greatest risk to critical operations. In a recent survey of 377 oil and gas security professionals, 65% of respondents said that a negligent or careless insider was their top cybersecurity concern, while 15% said it was a malicious or criminal insider. Overall, 59% of respondents said that OT is now a greater concern than IT.

Few companies in the oil and gas industry have taken the necessary steps to bridge the cyber readiness gap. Most lack a holistic cybersecurity strategy and have not dedicated sufficient financial or human resources to integrate cyber vigilance at all levels of their enterprises. This is particularly the case in the offshore environment, where the need to leverage digitalization and drive efficiencies is the most critical. Changing the status quo will require the industry to address the OT threat by adopting cyber best practices, such as:

Assign responsibility. Offshore, the responsibility of securing an oil and gas facility must fall on both the operator and asset owner. This is often not the case as companies operate in distributed environments with many suppliers where owners carry all the asset risk but do not run operations. Energy executives who want to demonstrate ownership will become more proactive in developing their own security measures rather than wait for these to be imposed on them from the outside.

Cyber transparency. Organizations cannot protect what they do not know they have. The only way to baseline OT risk is by creating an inventory of assets. As more and more legacy systems become connected and data gets pushed to the edge, prioritizing assets based on risk and business imperative becomes critical.

Hardening measures. Once assets have been prioritized, operators can take steps to deploy hardening measures – with the highest level of protection going to the most critical systems and the lowest level going to those that pose a less immediate risk to operations and safety. Additionally, some level of monitoring must be incorporated. In today’s environment, where the sophistication and complexity of OT attacks have reached machine speeds, the best strategies will be those that leverage machine learning and artificial intelligence (AI).

Incident response plan. Because it is impossible to prevent all cyber intrusions, it is crucial that operators have a plan in place to react to detected incidents. A successful reaction must quickly contain the attack and prevent further damage, and lead to implementing effective mitigating actions that prevent similar attacks from succeeding in the future.

Companies must embrace the idea that protecting their assets requires collaboration between industry and government and strengthening trust in the digital world. To achieve this, Siemens and several other global companies have initiated the “Charter of Trust.” The Charter of Trust calls for cybersecurity responsibility to be assumed at the highest levels of government and business and for companies to establish mandatory, independent third-party certification for critical infrastructure and solutions. The Charter has already been signed by the likes of Airbus, Allianz, IBM, MSC, NXP, SGS, and Deutsche Telekom, and represents an enormous step toward safely advancing digitalization in critical infrastructure operations.

Above all, it aims to create an industrial environment where cybersecurity is addressed proactively so that verticals, including oil and gas, can realize the full potential of digital transformation.

Leo Simonovich
Vice President and Global Head of Industrial Cyber and Digital Security, Siemens