Processing
SOLUTIONS FOR THE PROCESS INDUSTRIES®

6 reasons oil and gas organizations need to implement an industrial cybersecurity program

Oil and gas companies must focus on building robust industrial cybersecurity programs to prevent and respond to the next attack.

Ian Bramson

Over the course of the last year, a surge of unprecedented attacks has made industrial cybersecurity top of mind for industrial organizations around the world. This is particularly true in critical infrastructure sectors such as oil and gas.

Previously, cyber criminals concentrated their efforts on infiltrating the information technology (IT) networks that run business systems. However, they are now looking to disrupt the operational technology (OT) networks that control industrial operations. Threat actors have moved beyond stealing valuable data, to gaining control over entire market ecosystems.

The recent Colonial Pipeline incident demonstrates how hackers can wreak havoc when organizations assume IT threats will not impact OT. This ransomware attack was the strategic result of a password breach, which snowballed until OT operations were completely shut down. The consequence was a shortage of gasoline along the East Coast, pushing gas prices to their highest level in six years.

These dangerous breaches and the correlating ramifications are just beginning. In December of 2021, a detrimental cyber risk was identified in a widely used software called Java Log4j. Rated a 10 out of 10 on the vulnerability scale by the Cybersecurity and Infrastructure Security Agency (CISA), this threat has been labeled as one of the worst in history, with experts stating that organization's IT and OT networks worldwide are now at risk until further notice.

This breach, as well as the Colonial Pipeline shutdown, is not only a wake-up call for organizations, but for cyber criminals as well. Their impact on the nation's supply chain and economy has confirmed that the oil and gas

industry is a vulnerable and valuable target. Organizations must act now and prioritize the implementation of an industrial cybersecurity program to protect their operations, the environment and the community.

What makes oil and gas companies vulnerable to attacks?

There are several reasons oil and gas organizations are vulnerable to attacks, with the most critical being:

1. Lack of cybersecurity controls: The oil and gas industry does not have standard OT cybersecurity strategies and regulations, which has led to disparate and often inadequate security practices. Control systems run non-stop, day-in and day-out, leaving limited downtime for upgrades and updates, resulting in unpatched and inherently vulnerable OT systems.

Complicating matters even further is the fact that OT support in the oil and gas sector is inconsistent. Frequently, OT support relies on either IT teams who lack experience in OT cyber or operations teams who are at a disadvantage because they do not understand cybersecurity principles. Contrary to what many organizational leaders believe, IT solutions cannot simply be applied to OT systems because they do not translate. OT systems need specialized cybersecurity solutions and dedicated staff with OT expertise.

2. Remote capabilities are open to attacks: Today, many oil and gas organizations have dispersed assets and are heavily dependent on remote monitoring for management. While this connectivity offers many competitive advantages, it also creates vulnerabilities. Increased remote control over operations means more connection points for threat actors to break down organizational defenses and take control.

3. Growing operations are driving the expansion of attack surfaces: As oil and gas organizations expand their operations, the ways in which cyber threats can penetrate systems, also known as “attack surfaces,” are growing. Attackers are now trained to look for the cracks in these attack surfaces and exploit them.

4. Modern technologies pose new cyber risks: Digitalization, data analytics and automation are all competitive advantages. However, they pose new cyber risks. Many industrial environments are comprised of legacy systems that can be anywhere from 10 to 30 years old. These systems, given their age, were built for longevity, and not initially designed to be connected to wide area networks (WANs) or other modern technologies. These factors make them inherently vulnerable to attacks.

The combination of digitalization and an expanded attack surface creates additional challenges in managing cyber risk. When organizations centralize control and increase automation, analytics and data to gain a competitive advantage, the financial aspects often take priority, leaving OT cybersecurity tacked on as an afterthought. While high dependency on digitalization is only going to increase as it creates efficiencies, it also increases risk.

5. Attackers want more than data — they want physical control: Cyber attackers no longer just want to steal and manipulate data — they want direct control over the operations in physical environments where they can have the most impact. Attacks can now damage critical infrastructure, grind operations to a halt and

ultimately threaten national security by crippling essential industries like oil and gas. Something as simple as a password breach can disrupt the economy on a national scale and cause a ripple effect into adjacent industries.

6. Attackers are forming businesses: Although there are many distinct types of cyber attackers with different motivations, they all have started to form businesses around hacking. Their common thread is targeting industrial sectors like oil and gas, where they can have the biggest impact, disrupt business operations and make the most money.

Make OT cybersecurity a priority

Organizations must be proactive when it comes to securing their OT systems and understand that it is not enough to patch the vulnerability that led to the last high-profile attack. Since attackers are highly adaptable and constantly evolving, oil and gas companies must focus on building robust industrial cybersecurity programs to prevent and respond to the next attack. It is vital to prepare for *when,* not *if* an attack occurs.

The most successful organizations will work to develop a framework to identify potential weaknesses, protect against attacks, detect attacks when they occur, respond quickly and recover effectively. Taking a proactive approach will make an organization resilient to future attempts and give peace of mind in a quickly changing environment.

Ian Bramson is Global Head of Industrial Cybersecurity at ABS Group and a recognized leader in the emerging threat landscape of attacks on industrial operations and critical infrastructure. With more than 20 years of experience in cybersecurity and technology, Ian works directly with executives in the energy, industrial and maritime sectors to help minimize their cybersecurity risks.