6 reasons chemical organizations need to implement an industrial cybersecurity program now

In the last year, a surge of unprecedented cyber-attacks has thrust industrial cybersecurity into the spotlight, making it a top priority for organizations around the world.

This is particularly true for businesses within critical infrastructure sectors like oil, gas and chemical. Threat actors have moved from stealing valuable data to attacking operation technology (OT) networks, allowing them to gain control over entire market ecosystems.

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

This breach was not only a wake-up call for organizations but for cybercriminals as well. The impact on the nation's supply chain and economy confirmed that critical infrastructure is a valuable target—and a vulnerable one. Organizations must prioritize the implementation of industrial cybersecurity programs if they want to protect their operations, the environment, and their communities.

What Makes Chemical Companies Vulnerable to Attacks?

1. Lack of cybersecurity controls: The chemical industry does not have standard OT cybersecurity strategies and regulations. This has led to companies having disparate—and often inadequate—security practices. Furthermore, OT support too often relies on existing teams ill-equipped to meet the needs of an OT program. IT professionals either lack experience in OT cyber or operations teams 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. They require specialized cybersecurity solutions and dedicated staff with OT expertise.

2. Growing operations drive the expansion of attack surfaces: As chemical 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 exploit the cracks found in these larger attack surfaces.

3. Remote capabilities are open to attacks: Today, many chemical organizations have dispersed assets and are heavily dependent on remote monitoring for management. While this connectivity offers many competitive advantages, it also creates vulnerabilities. Each remote device is a possible point of failure. As these ecosystems grow, so too does risk.

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 decades-old legacy systems. These systems were built for longevity—but they were not designed to be connected to wide area networks (WANs) or other modern technologies. This makes them vulnerable to attack.

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 physical environments. Attacks can now damage critical infrastructure, grind operations to a halt, threaten national security and put lives at risk by crippling essential industries.

6. Attackers are forming businesses: Although there are many distinct types of cyber attackers with different motivations, they have started to form businesses around hacking. While terrorists and hacktivists may not be working with each other, these groups are forming alliances with other individuals who share their values to broaden their reach and expand their capabilities.

Make OT Cybersecurity a Priority

Organizations must understand that patching the vulnerability that led to the last high-profile attack is not enough. Since attackers are highly adaptable and constantly evolving, chemical companies must focus on building robust industrial cybersecurity programs that take a proactive approach to security. It's vital to prepare for when, not if, an attack occurs.

The most successful organizations develop a framework early. It should include processes for identifying weaknesses, protecting against attacks, detecting attacks when they occur, responding quickly and recovering effectively. Taking a proactive approach will make an organization resilient to future attempts and provide peace of mind in a quickly changing environment.

Ian Bramson, Global Head of Industrial Cybersecurity at ABS Group, USA