The Chemical Industry and the Rise of Cybersecurity Risk

The Colonial Pipeline shutdown has significantly impacted enterprise functions, critical infrastructure and industrial operations, forcing substantial parts of the pipeline to shut down for several days.

This cyber attack has far-reaching implications not only in the oil and gas market but across several industries, including oil, gas and chemicals, among others. This strategic attack is an example of how cyber criminals can swiftly disable operations and effectively impact businesses, the public and a Nation's economy.

As companies recover from the attack, business leaders are correctly asking the question: Is this the new normal? No industry is safe in a world where connectivity drives business and the chemical industry presents an especially attractive target for cyber criminals for the high impact a cyber attack can have on public safety and operations.

Market changes are increasing vulnerability

Three fundamental shifts in the market have led to this vulnerability.

First, cyber criminals have begun to move their attacks from traditional Information Technology (IT) networks – those made up of the servers, computers and mobile devices that enable business operations – to Operational Technology (OT) targets, which are the machines, systems and networks that are directly used at plants and in operations. Essentially, these are physical infrastructures and digital inputs that make manufacturing and business happen.

OT is a new kind of prize. Instead of stealing and manipulating data, cyber attackers now want to take direct control of your operations. This includes shutting down, over-speeding, overloading and disrupting networks, systems and equipment fundamental for your daily operations. When exploits occur at any point on the OT network, threats can easily spread to other devices. Industrial cybersecurity is now an operational and safety risk.

Second, many chemical companies are embracing digitalization of their operations. Digitalization promises significant increases in efficiency and profitability through the modernization of technology, advanced analytics and automation. Although it represents a competitive advantage in the market, it also brings new cyber risks. Connectivity increases as more sensors, devices and the Industrial Internet of Things (IIoT) are added to the operational network. This expands the points-of-exploitation for attackers.

Third, cyber attackers are realizing that OT systems present the ability to have critical impacts. They can expand from not only stealing, disrupting and destroying data, to directly impacting critical operations and safety. These not only raise the profile of their attacks but increase the profitability and value of their exploitations.

What you can do

Basic cyber hygiene can go a long way to reduce your industrial cyber risk. Here are some cyber basics to keep in mind:

- **Take industrial cyber seriously** – Industrial cybersecurity is a business imperative. It is as important to your growth as any strategic investment. Make sure you have the program, investment and capabilities in place to minimize your OT cyber risk.
- **Know what to protect** – Make sure you have a robust and automated asset inventory and management system. This will let you know what you need to protect, and what systems are connected.
- **Manage your vulnerabilities** – Once you know what to protect, know the holes in your defenses. Prioritize those holes and close them.
- **Cyber starts from the beginning** – Cyber begins from the concept phase. Make sure security-by-design and supply chain risk management is a core part of your new construction and expansion.
- **It's about visibility and control** – Make sure you have a robust monitoring and response program. Without these, you're flying blind.
- **Find the right partner** – Industrial cyber is a challenge. It takes domain expertise and a solution built specifically for the OT environment. OT cyber is likely not your core business. Find a partner who has the experience and expertise in OT cyber to minimize your risk.

By Ian Bramson
Global Head of Cybersecurity

ABS Group of Companies, Inc.
1701 City Plaza Drive
Spring, TX 77389 USA
Tel: 1-281-673-2800
Fax: 1-281-673-2900
www.abs-group.com