Nexus Controls
a Baker Hughes business

Blog

Connectivity is bringing industrial cybersecurity threats closer than ever—here's how to protect against them

Chad Elmendorf
Sr. Global Product Marketing Leader

The industrial sector is in the midst of a transformation driven by disruptive technologies such as the Industrial Internet of Things (IIoT), robotics, virtual reality (VR) and artificial intelligence (AI) that is changing the way we produce, work, distribute, and live. It's called the fourth industrial revolution (4IR) due to the incredible impact it has already had and will continue to have on industry around the world.

At the heart of the 4IR is connectivity between operational technology (OT) and information technology (IT). Industrial assets, which were once physically separate from networks, are now connected remotely to potentially vulnerable IT systems. For example, more and more oil and gas organizations are using remote operations from an onshore location or nearby platform via shared computer networks.

Digitizing factories provides many benefits including a united, single pane view of operations and enables enterprises to remotely improve operational efficiency, production quality, employee safety, and machine health. It also exposes key IT vulnerabilities that attackers are already taking advantage of. In order to maintain robust optimal production, companies must take proactive steps to protect against lurking cybersecurity threats, particularly from legacy systems and outdated operating systems running in plant networks.

Key industrial cybersecurity vulnerabilities

Legacy assets are at the epicenter of industrial digital transformation. They control critical operational processes, but the cybersecurity of these assets and the networks they reside is often lacking. As those assets are equipped with IIoT sensors and connected to facility industrial control systems (ICS), security teams are encountering challenges in ensuring that both the critical equipment and the enterprise network are protected against threats.

Adding further complication, most of the industrial control systems currently in operation were designed prior to the digital era. Frost & Sullivan research conducted in partnership with Baker Hughes indicates the relative shelf asset lifecycle of controllers is approximately 15 years, and the average age for most industrial control environments today is an estimated 20 years. Obsolescent legacy infrastructures have not commonly been refreshed or hardened with cybersecurity capabilities or solutions. This creates vulnerabilities that can be targeted by cyber-attacks or exacerbated by human errors.

As industry becomes more sophisticated, so too are the hackers targeting industrial plants and networks. Targets are being selected well in advance with specific goals in mind. Furthermore, today's attackers are doing their homework and have often gained intimate knowledge of their targets via public records and available company data.

Syndicated reports worldwide indicate lack of cyber-preparedness, an increase in attacker sophistication, and a significant uptick in the number of attacks on critical infrastructures. For instance, a 2018 technical alert issued by the U.S. Department of Homeland Security describes a sophisticated attack targeting Energy and other Critical Infrastructure sectors.

As shown in this image, there are four key areas of vulnerability that the industrial enterprise must address.

A single weak security point creates an opening for cyber-attackers to access a plant and its sensitive data. Unfortunately, most organizations are still waiting to act until after an attack has already occurred. Detecting and preventing cyber-attacks is far more cost-effective for organizations than taking corrective actions after the fact. As the saying goes "an ounce of prevention is worth a pound of cure". While it's impossible to address all cyber risks, organizations must make informed decisions on which threats are most likely and optimize resource allocation to effectively reduce risk to an acceptable level.

Leveling the cybersecurity landscape

Effective protection against sophisticated threats requires that organizations become equally sophisticated with their approach to cybersecurity. Although not all cyber risks can be eliminated, synchronized countermeasures provide companies with the ability to mitigate a significant portion of their enterprise risk.

Setting specific target goals and understanding how long it's going to take to accomplish them are two of the key foundations of a successful security strategy. For example, OT updates typically are implemented during pre-scheduled outages, so changes to secure the network may need to wait longer than IT updates in the energy industry as facilities often operate 24/7.

Systematic assessments of vulnerabilities enable firms to minimize ICS security risks. Formulating a plan for what to do in the event of an attack empowers an efficient response and minimizes damage. Here are some key steps organizations can take to help level the cybersecurity landscape:

- Change default credentials immediately
- Understand normal ICS network operation to determine when "abnormal" occurs
- Continuously monitor and regularly patch installed software and operating systems
- Use the same reconnaissance tools the attackers are using (Shodan is one example) to check for vulnerabilities
- Make cybersecurity a business strategy
- Leverage a trusted cybersecurity partner with deep OT domain expertise

A trusted cybersecurity partner can help identify and mitigate threats within an industrial facility or across a multi-site network. Furthermore, companies can leverage partner expertise to level-up the knowledge of their own team members. Outsourcing some or all of cybersecurity protection helps in three key ways:

1. **Reduces labor costs and resources:** leveraging the expertise and protection resources of a partner frees company team members to focus on other day-to-day priorities, saving time and money.
2. **Strengthens overall security posture:** cybersecurity solution providers that can deliver comprehensive solutions rather than "point products" offer greater enterprise-wide visibility and protection. Virtualization and strong access management allow traceability on activities.
3. **Ensures regulation compliance:** as cyber regulations continue to evolve and mature, it is important to work with an organization that has the ability to stay ahead of the market while understanding the nuances of operational technology cybersecurity.

The industrial cyber threat landscape is very real but it's possible to take steps to identify vulnerabilities and reduce risk. A proactive strategy can help keep operations running, reduce unexpected costs, and keep personnel safe.

Download the **Securing with Trust to Achieve Cybersecurity Peace of Mind** whitepaper today to learn how to properly protect your operations—today and as we journey forward together into the future.

I would love to hear how you're thinking about threats to your OT network in the comments. Together, we can help secure the world's critical infrastructure.

You produce. we Protect.

Nexus Controls
a Baker Hughes business