Nexus Controls
a Baker Hughes business

Blog

Getting serious about cybersecurity in the oil and gas industry

Chad Elmendorf
Sr. Global Product Marketing Leader

Digital transformation has the promise to positively change business outcomes across multiple industrial sectors including the Oil & Gas industry. With the rise of software-based connectivity, the separation between information technology (IT) and operational technology (OT) networks is shrinking. Legacy equipment that used to be monitored by handheld equipment and standalone sensors is now being integrated into the connected enterprise network to gain valuable insights from machine data.

The modern, connected factory is advancing operational productivity and efficiency– but without an effective cybersecurity strategy, enterprise risk can increase significantly. As IT and OT networks converge, facilities must adopt a system of cybersecurity protection to ensure equipment and personnel safety. Legacy equipment is particularly vulnerable since it's often responsible for the most critical functions in an O&G facility but often lacks even the most basic protections.

Opportunities often add risk exposure

Nexus Controls, a Baker Hughes business held a webinar focused on Industrial Cybersecurity in the Oil & Gas industry we outlined the threats O&G operators currently face and the necessary steps that must be taken to develop an effective cybersecurity strategy.

IT/OT convergence is proving that there is significant business value to be realized in the Oil & Gas sector. The results of one Bain study revealed that IoT data analytic insights can help improve O&G production by as much as 6% to 8%. Leveraging IIoT technology, it's possible for to tap into the enterprise network to understand how an individual drill operation hundreds of miles away may affect vendors upstream, ultimately providing a more complete picture of the value chain. This unprecedented connectivity is the same exposure that attackers are now taking advantage of.

But, as the industry becomes more sophisticated, so too are the attackers targeting industrial networks. Targets are being selected with specific goals in mind. Furthermore, today's attackers are often well-funded and have researched their targets well via public records and available company data, and other sources.

Some key vulnerabilities within the OT space include:

- Windows operating system controllers
- Legacy systems since they're difficult to update and patch
- Third party vendors given service access and not revoked after service is completed
- Dual-homed devices that can tap into the enterprise network outside the facility
- Unknown risk areas due to unprotected or poorly segmented assets

The answer is relatively straightforward, but risk-based implementation is much more difficult. With an effective cybersecurity strategy, it's possible to mitigate many threats and reduce risk to an acceptable level.

Here are some top tips to protect against today's attackers:

- Change default credentials immediately
- Understand normal ICS network operation to determine when "abnormal" occurs
- Continuously monitor and patch OT assets
- Use the same reconnaissance tools the hackers are using (Shodan is one example) to check for vulnerabilities
- Make cybersecurity an evolving business strategy

Security is a business decision

Protection against sophisticated attacker threats requires that organizations become equally sophisticated with their approach to cybersecurity. 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, in downstream refineries, OT updates typically work around outage schedules so changes take much longer to implement in the Oil & Gas industry since facilities often operate 24/7.

Threats are constantly evolving and administering a culture of continuous improvement is one key step toward adopting a cybersecurity strategy that really works. Organizations should remember to:

1. Define and routinely adjust your cybersecurity roadmap
2. Set priorities based on risk
3. Build protection toward top threats
4. Leverage trusted cybersecurity partners

As the Oil & Gas industry undergoes digital transformation, attackers are eager to target critical high-value facilities and assets. The right cybersecurity partner monitors threats 24/7 and can help facilities proactively eliminate vulnerabilities – long before a breach occurs.

To learn more, listen to our on-demand webinar Latest threats to the Oil & Gas Industry and how your cybersecurity strategy needs to adapt.

Check out our full portfolio of cybersecurity solutions today.

You Produce. We Protect.

Download the whitepaper here

Nexus Controls
a Baker Hughes business