Baker Hughes

How to protect against cybersecurity threats in the oil & gas industry

"Don't think you're not a target. Everyone is vulnerable, no matter how small."

Derek Bourland, Senior Product Manager – Cybersecurity, Nexus Controls, a Baker Hughes business

Adversaries are well funded, motivated, and are in it for the longterm.

Cybersecurity incident outcomes:

- Safety issues
- Production downtime
- Physical asset damage
- Sub-standard output quality
- Regulatory liabilities

Attackers research and study their targets infrastructure's prior to launching a attack

Oil & gas targets chosen with specific goals

Attackers look for unprotected IOT devices in connected sites

Key vulnerabilities in OT networks

- Default credentials
- Legacy systems since they're difficult to update and patch
- Third party vendors given service access and not revoked after service is completed
- Public information about cybersecurity protections in place (i.e. job listings)
- Dual-homed devices

Top tips to protect against hackers

- Change default credentials immediately
- Baseline normal ICS network operation to determine when "abnormal" occurs
- Continuously monitor and patch IT vulnerabilities
- Make cybersecurity a business strategy

Protect your industrial network

Define roadmap

Set priorities based on risk

Build protection toward top threats

Leverage trusted cybersecurity partners

Contact us to learn more about how Baker Hughes leverages more than a decade of cybersecurity experience to effectively mitigate cyber vulnerabilities and risk.

bakerhughesds.com/cybersecurity

You Produce. We Protect.