

Checklist: Securing Your Critical Infrastructure

Pipeline operators, energy companies, and government agencies face mounting cybersecurity threats that have exponentially multiplied. And whether it's a time-crunch TSA security directive on oil and gas companies, a shift to remote work, or a ransomware attack — organizations are more compelled than ever to fortify their security programs.

Use this checklist to conduct a preliminary evaluation of your organization's security posture — and start charting a path to more fully developed cybersecurity strategies.

Ensure complete visibility into the IT environment.

- Create transparency across every facet of the network infrastructure, including:
 - Vulnerabilities
 - Activities
 - Network users/user groups



Adopt a governance framework.

- Outline responsibilities.
- Assign roles.
- Align security decisions with business strategies, requirements, and objectives.



Modernize identity and access management.

- Migrate to a Zero Trust strategy, including:
 - Cloud-based Single Sign-On (SSO)
 - Multi-Factor Authentication (MFA)



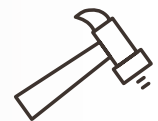
Automate and streamline.

- Reduce noise and alert fatigue.
- Refocus resources on critical threat hunting and investigation.



Lean on proven tools and outside help.

- Consider consolidating tool sets.
- Adopt multiplatform security tools that provide:
 - Improved visibility
 - Enhanced automation
 - Artificial intelligence- and machine learning-powered capabilities



A partner for excellence in infrastructure security

Insight provides a holistic, programmatic approach to identifying security gaps, providing recommendations, and helping implement and manage security solutions. Not only do we offer assessments and solutions to help support compliance — we can also help with identifying and leveraging government and partner funding available for compliance-related security initiatives.

Interested in working with Insight? Let's connect.

Visit insightCDCT.com/contact-us to get started.