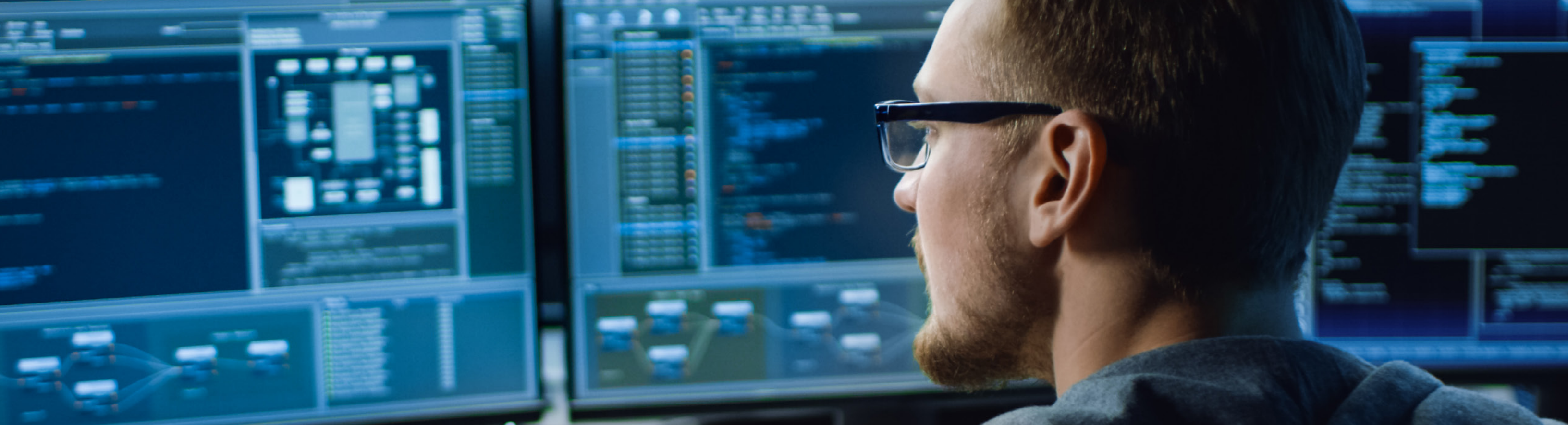
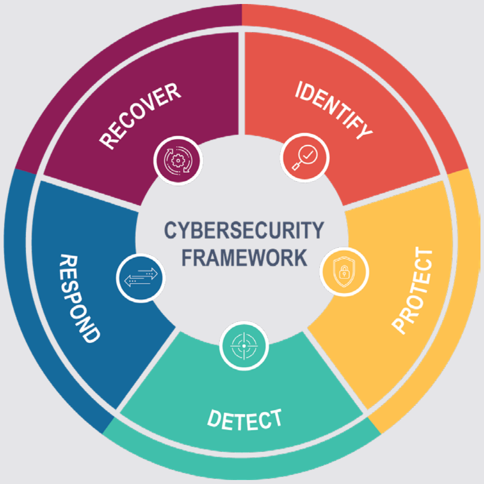


CYBERSECURITY RISK ASSESSMENT

Uncover Hidden Threats With a Cybersecurity Risk Assessment

Are you confident that your industrial facility is adequately protected against the growing threat of cyber-attacks? At Interstates, we understand the critical importance of safeguarding your industrial facility's infrastructure from cyber threats. Conducting a cybersecurity risk assessment is an integral part of achieving this goal. By identifying vulnerabilities in your Operational Technology (OT) systems, our assessment enables proactive steps to address them and prevent exploitation by cyber attackers.

Our holistic approach evaluates the interplay between people, processes, and technology within facility operations, offering a comprehensive understanding of the cybersecurity landscape. We also emphasize the importance of creating a culture of cybersecurity, where employees play a vital role in protecting the company from security breaches. With our specialized expertise, experienced staff, and well-established process, we deliver thorough assessments tailored to your needs, providing clarity and confidence throughout the assessment journey.



Why Conduct a Cybersecurity Risk Assessment?

IDENTIFY VULNERABILITIES

Reveal OT vulnerabilities, thwarts cyber attackers, and ensure system protection.

MITIGATE RISKS

Gain insights into OT risks to implement tailored cybersecurity controls: policies, upgrades and training for resilience.

ENSURE BUSINESS CONTINUITY

Fortify against cyber risks, ensure operational stability and minimize impact.

The Process

Our exceptional expertise in comprehensive company-wide control system cybersecurity assessments sets us apart. With certified professionals experienced in both OT and IT domains, we bring extensive knowledge to deliver tailored and thorough assessments for our clients.

1. **Discovery** - Understanding the goals you have for your assessment and developing your proposal.
2. **Site Assessment** - During this time, we'll prep for our on-site visit, conduct the on-site work and record findings.
3. **Analysis** - We'll take a few weeks to review our findings and then provide you with a prioritized list of recommendations.
4. **Results** - After you've seen the report, you will have a chance to ask questions about our findings and address any additional needs.

What You Get

Our assessments are based primarily on the Cybersecurity Framework (CSF) developed by the National Institute of Standards and Technology (NIST). Beyond assessing the OT environment to understand compliance levels with NIST CSF, Interstates also assesses the adequacy of the implementation of controls. This allows us to provide guided recommendations to improve your cybersecurity stance.

AREAS OF REVIEW

| Asset Inventory
| Risk Management
| Network & Information Design
| Personnel
| Access Control
| Backup Management
| Business Continuity
| Preventative Measures
| Business Partners
| Technology Outlook
| Threat Protection
| Other (additional areas you identify as important)

Ready To Get Started?

If you are ready to safeguard your facility with our comprehensive assessment, or need more information, contact OTIS@interstates.com or reach out to your Interstates representative.