Cybersecurity

The Problem and Its Solutions

Cybersecurity in the U.S

National Cybersecurity Strategy:

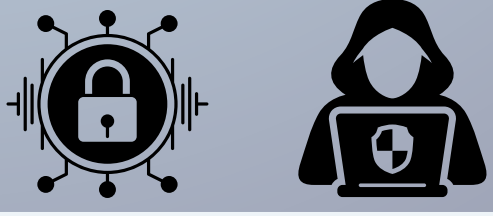
- Cybersecurity is a national security priority
- Five goals:
  - Protect critical infrastructure
  - Secure federal networks
  - Build a more secure and resilient internet
  - Improve the cybersecurity workforce
  - Promote responsible behavior in cyberspace
- Outlines a comprehensive approach to improving national cybersecurity
- Highlights the need for collaboration, innovation, and partnership to address the evolving threats and challenges in cyberspace

What is Cybersecurity?

Cybersecurity is the practice of protecting systems, networks, and data from digital attacks.

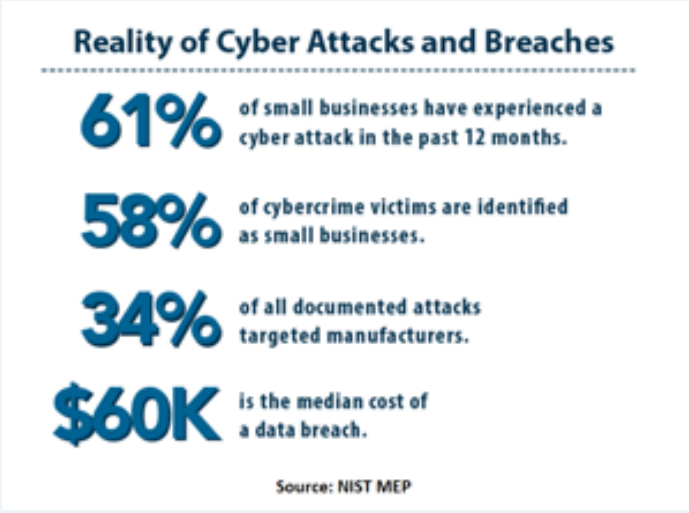
As systems to control energy-using manufacturing equipment become more connected to the internet, it is important for plant operations staff to have an understanding of cybersecurity risks and to coordinate risk management activities within their organization.

Industrial Assessment Centers work with manufacturing clients to increase awareness of cybersecurity risks and potential mitigation activities. As part of facility site visits, IAC clients may elect to receive cybersecurity risk assessments to identify security and privacy deficiencies to the business infrastructure, with a focus on vulnerabilities associated with industrial controls systems.



Why is it important?

Small businesses may not consider themselves targets for cyber-attacks. However, they have valuable information cyber criminals seek, such as employee and customer records, bank account information, and access to larger networks. They can be at a higher risk for cybersecurity attacks because they have fewer resources dedicated to cybersecurity. By addressing risk areas, you can protect your business from damage to information or systems, intellectual property theft, regulatory fines/penalties, decreased productivity, or a loss of trust with customers.



- The IAC Industrial Control Systems Cybersecurity Assessment Tool features 20 questions to evaluate industrial controls systems and plant operations, providing a risk assessment (high, medium, or low).
- The User Guide offers context for these questions, helping clients understand how certain practices contribute to cybersecurity risks.
- After the assessment, the tool generates a customized list of action items based on identified risks. For further guidance, IACs direct clients to additional resource materials from the NIST Manufacturing Extension Partnership (MEP) and other organizations.

The best way to improve cybersecurity is to have a risk assessment completed.

Benefits of a risk assessment

- Identify vulnerabilities
- Improve security posture
- Ensure regulatory compliance
- Risk management
- Build customer trust
- Cost savings

Negative effects of a cybersecurity attack

- Financial Loss
- Reputation Damage
- Legal and Regulatory Consequences
- Operational Disruption
- Investor and Partner Relations
- Supply Chain risk

Additional Resources

- *https://iac.university/cybersecurity*
- *https://iac.msu.edu/cybersecurity/resources*
- *Cyber Security Evaluation Tool (CSET):* Comprehensive desktop software tool that guides users through a step-by-step process to assess their control system and information technology network security practices against recognized industry standards.
- *NIST MEP Cybersecurity Assessment Tool:* Online easy-to-use checklist that provides an assessment of business systems.
- *Department of Energy C2M2 Model:* Model used to measure the maturity of an organization's cybersecurity capabilities, developed by energy sector subject matter experts.
- *Department of Homeland Security Cyber Resilience Review:* No-cost, non-technical assessment to evaluate an organization's operational resilience and cybersecurity practices.
- Michigan Manufacturing Technology Center
- University of Michigan's Advanced Manufacturing Cybersecurity Program

Fundamentals

Most plant operations managers are not cybersecurity experts but can benefit from a basic understanding of cybersecurity risks and mitigation activities. **NIST Small Business Information Security: The Fundamentals**, provides a thorough and easily readable overview of cybersecurity basics.

- Identify what information your business stores and uses.
- Determine the value of your information.
- Develop an inventory of technologies used to store and process information.
- Understand your threats and vulnerabilities.

Source: N. Hanacek/NIST

Cybersecurity

The Problem and Its Solutions