

# CYBERSECURITY 5-MINUTE STUDY GUIDE

According to the U.S. Department of Homeland Security, the manufacturing industry is the second most targeted industry based on the number of reported cyber-attacks. Strengthening your strategy here directly protects your bottom line.

This quick guide provides the basics to get you grounded and curious to dig deeper. Dive in, and let's get the ball rolling on your journey to mastering cybersecurity!



## WHAT IS CYBERSECURITY?



- Cybersecurity is the **safeguarding of digital information** and systems from unauthorized access, theft, or damage.
- It encompasses the **protection of your business's vital components, reputation, and relationships** with suppliers and customers.
- Implementing a proactive, balanced strategy for addressing potential issues before they arise **offers a competitive edge**.
- Importantly, cybersecurity is **a collective responsibility**, not solely the task of the IT Department. Much like the diligence exercised in locking a door to secure physical premises. Sometimes it is the simple things like not leaving a written down password on your desk or locking your computer. The everyday practice and knowledge of fundamentals play a key role in the safety of your business.

## CORE PRINCIPLES

- **Confidentiality:** Ensuring only authorized individuals access information.
- **Integrity:** Maintaining accuracy and completeness of data.
- **Availability:** Ensuring reliable access to information when needed.

## TOOLS & TECHNIQUES

- **Firewalls and Antivirus:** Preventing unauthorized access and detecting malware.
- **Encryption:** Scrambling data to protect its confidentiality.
- **Intrusion Detection Systems (IDS):** Monitoring network or system activities for malicious activities or policy violations.
- **Secure Sockets Layer (SSL)/Transport Layer Security (TLS):** Protocols for establishing authenticated and encrypted links between networked computers.

## KEY METHODOLOGIES

- **Risk Management:** Identifying, assessing, and mitigating risks to digital assets.
- **Incident Response:** Preparing for and responding to cybersecurity incidents.
- **Authentication & Access Control:** Verifying user identities and managing access to resources.
- **Threat Intelligence:** Gathering and analyzing information about emerging or existing threats.

## PERFORMANCE METRICS

- **Incident Detection Time:** Speed in identifying security breaches.
- **Compliance Rate:** Adherence to cybersecurity policies and standards.



These short study guides are a concise introduction to topics that enhance efficiency, security, and team dynamics. **Dive in with these bite-sized learnings** to get to know the terms, tools and topics that can drive success and innovation in your manufacturing processes!

**Want more information? Contact us today!**

<https://vmec.org/contact/>



## RESOURCES



**Cybersecurity & Infrastructure Security Agency (CISA)** has compiled a list of free services and tools provided by private and public sector organizations across the cyber community:

<https://www.cisa.gov/resources-tools/resources/free-cybersecurity-services-and-tools>



**NUARI has launched the Norwich University Applied Research Institutes Resource Library** to help individuals and organizations find resources they can use and share. This library features free and updated information on current cybersecurity, critical infrastructure resilience, defense technologies, information warfare and more:

<https://nuari.org/resource-library/>

## WHAT WE DO

We offer a suite of services to enhance cybersecurity and supply chain management. Our approach includes evaluating your current systems to identify any gaps or vulnerabilities, developing frameworks to bolster organizational resilience against cyber threats, and providing education and training to meet compliance standards.

### Services Tailored to Your Needs:

- Cybersecurity assessments and gap analyses
- Organizational resilience framework development
- Cyber competencies education and NIST compliance training
- Tailored cyber exercises and secure network monitoring

Together with our partner NUARI, a 501(c)(3) non-profit that serves the national public interest through the interdisciplinary study of critical national security issues, **we will develop a cybersecurity plan based on your organization's current state.**



### BRETT FERENCE

Director of Business Development

**Need help or want to dive deeper? Contact Brett!** Brett has extensive experience developing and managing product lines around the globe

(802) 779-2709 • [bference@vmec.org](mailto:bference@vmec.org)