

# INTELLIGENT MANUFACTURING SYSTEMS

Global Research and Business  
Innovation Program



IMS INTERNATIONAL  
+1 844-446-7676  
[www.ims.org](http://www.ims.org)

## Cybersecurity





# Cybersecurity

## How to Use This Guidebook

Each Cybersecurity Guidebook is created with the business growth needs of small and medium manufacturers in mind. By utilizing the information in this guidebook, you are taking the first steps to creating a competitive advantage for your company by innovating in the face of disruptive technologies.

This guidebook follows a logical flow to guide you as you learn more about Cybersecurity (see Fig. 1). Review the sections as they apply to your individual opportunities and resources, either in the order they're presented or jump around to fit your immediate needs.

*Figure 1: Cybersecurity Guidebook Information Flow*



This is your toolkit for plugging into the Cybersecurity platforms innovation network.

Together, all of our guidebooks work to uplift manufacturers through increasing digital readiness; working together to accelerate the understanding and investment in emerging technologies; and foster a culture of innovation in the manufacturing industry. We encourage you to also review the other guidebooks in this series.

## Who can I contact at IMS?

### **Dan Nagy**

Managing Director  
IMS Inter-Regional Secretariat  
ph: +1 844-446-7676  
dnagy@ims.org  
www.ims.org

### **Teresa Morin**

Special Projects Manager  
IMS Inter-Regional Secretariat  
ph: +1 844-446-7676  
teresa.morin@ims.org  
www.ims.org



# Cybersecurity

## Cybersecurity at a Glance

### What does Cybersecurity encompass?

Wikipedia has a simple definition: Cybersecurity is the protection of computer systems from the theft or damage to their hardware, software or information, as well as from disruption or misdirection of the services they provide.<sup>1</sup> What is difficult to grasp is the scope. Cyber-attacks threaten all businesses from personal computers to large organizations. Virtually everyone is vulnerable regardless of their business size, the sophistication of their systems, or connectivity to a network. Every single digital device is a target.

### Why does Cybersecurity matter to your business?

Cybersecurity is a shared responsibility among suppliers. Many manufacturers interact with large customers or they do business with the Department of Defense (DoD). These organizations are constantly raising the bar requiring that their suppliers' systems are adequately protected. Why? Because criminals find the weakest link, and once one system is compromised it moves around the supply chain leading to data theft, corruption, and business disruption. You can create a competitive advantage by being known as a leader in Cybersecurity and a place in the supply chain where customers have confidence that their data and systems are safe.

Regulation deadlines will impact many businesses that are not even aware that they could become noncompliant. The DoD required suppliers to reach NIST/DFARS 800-171 compliance by Dec. 25, 2017, and if they do not comply they may face fines or loss of DoD business. The Special Publication outlining the new requirements can be found at: <http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171.pdf>

### What are the biggest opportunity areas?

We have identified three key opportunity areas in Cybersecurity for manufacturers. More information can be found in the Identify Opportunities section on pg. 8.

**Opportunity #1:** Protect your company's data and systems. Understanding and mitigating risks reduces the likelihood of and damage associated with a breach.

**Opportunity #2:** Minimize the impacts of an incident. Proactively planning for an incident increases your ability to detect, react, and recover, greatly reducing the cost associated with each occurrence.

**Opportunity #3:** Gain competitive advantage as a secure partner. As you work to meet industry standards or become NIST certified, your customers will gain confidence in your capability to be a trusted partner in the supply chain, turning Cybersecurity into a competitive advantage for your company.

<sup>1</sup> [https://en.wikipedia.org/wiki/Computer\\_security](https://en.wikipedia.org/wiki/Computer_security)



# Your CYBERSE

## **What are the business benefits of a Cybersecurity program?**

The business benefits of a Cybersecurity program can be very impactful. <sup>2</sup>

- Protect your business from disruptions of operations
- Protect your company's brand and reputation
- Avoid lost sales, fines and legal costs
- Faster recovery times in case you have a breach

Cyber-crime costs are predicted to hit \$6 trillion annually by 2021.<sup>3</sup> Most people have a personal experience or know someone who has gone through and horror of dealing with a personal or company breach. Loss of productivity, damaged company image, consulting fees, and financial losses are among the ruins. These costs are real and can be devastating to a company. Being cyber secure and keeping your business safe is a fundamental responsibility of every business owner and leader.

## **Where can I find help to get started?**

There are resources that can assist you with the development and implementation of Cybersecurity program. There are also many free online resources, as well as educational courses offered by universities and colleges. Turn to page 20 for a full list of resources to jump start your Cybersecurity journey.

<sup>2</sup> Per Quad Cities Cybersecurity Alliance

<sup>3</sup> <https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/>





# Cybersecurity

## Table of Contents

<b>How to Use This Guidebook</b>	2
Whom can I contact with questions?	2
<b>Cybersecurity at a Glance</b>	3
What does Cybersecurity encompass?	3
Why does Cybersecurity matter?	3
What are the biggest opportunity areas?	3
What are the business benefits of a Cybersecurity program?	3
Where can I find help to get started?	4
<b>Table of Contents</b>	5
<b>Understand the Technologies</b>	6
Additional Online Resources	8
<b>Identify Opportunities</b>	8
Opportunity #1: Protect Your Company's Data and Systems	8
Opportunity #2: Minimize Impacts of an Incident	9
Opportunity #3: Gain Competitive Advantage as a Secure Partner	9
Benefits and Use Cases of Cybersecurity Opportunities	9
<b>Build the Business Case and Begin Implementation</b>	10
Change Management: Building the Case Requires a "Test-and-Learn" Approach	10
Processes and Frameworks for Implementing Cybersecurity	11
The Basic Business Benefits	12
DFARS Certification	12
Calculating ROI	13
Establishing or Improving a Cybersecurity Program	13
Resources Needed: Technology and Staffing	15
"Quick Wins" to Get Started with Cybersecurity	18
Metrics for Success: How to Measure Impact	19
<b>Find Help with Assets &amp; Partners</b>	20
<b>Appendix: Glossary - Cybersecurity Terms</b>	21



To Continue Reading Please Log Into Your  
IMS.org Account and Go to [Member Resources](#).

All those residing in the United States, South Africa, and  
Mexico (Pending) are eligible to create an account.

For more information on IMS membership please email  
[dnagy@ims.org](mailto:dnagy@ims.org).