Quad Cities Manufacturing Innovation Hub Playbook Series
Cybersecurity

How to Use This Playbook
Each Quad Cities Manufacturing Innovation Hub playbook is created with the business growth needs of our area’s small and medium manufacturers in mind. By utilizing the information in the Cybersecurity Playbook, you can be confident that you are taking the right steps to protect your company and preparing yourself to safely leverage emerging digital technologies.

This playbook 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 Playbook Information Flow

This is your toolkit for plugging into the cybersecurity network in the Quad Cities.

Together all eight of our playbooks uplift our regional manufacturers and Department of Defense suppliers through increasing digital readiness, working in concert to accelerate the understanding and investment in emerging technologies and to foster a culture of innovation in the manufacturing industry. We encourage you to review the other playbooks (see appendix for more information) as well.

Whom can I contact at the Quad Cities Manufacturing Innovation Hub with questions? Email askthehub@quadcitieschamber.com, and a member of the Hub team will respond to your question.

About the Quad Cities Manufacturing Innovation Hub and Our Partners
The Quad Cities Manufacturing Innovation Hub assists businesses by offering services such as operational assessments, registry in a regional catalog of manufacturers and suppliers, trade and business-to-business events, access to national marketing, access to subject matter experts through the Chamber’s Critical Talent Network, connections to the Quad City Manufacturing Lab and national research, and training seminars targeted at key technologies. More information on the Hub can be found online here.

This content was prepared as part of the Illinois Defense Industry Adjustment Program, a partnership between the University of Illinois System, the Quad Cities Chamber of Commerce, and the Voorhees Center at the University of Illinois Chicago (UIC), with financial support from the U.S. Department of Defense, Office of Economic Adjustment (OEA). It reflects the views of the Quad Cities Chamber of Commerce and does not necessarily reflect the views of the OEA. For more information, please visit www.IllinoisDIA.org.
Cybersecurity in the Quad Cities: 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.\(^1\) 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 the Quad Cities community?
Cybersecurity is a shared responsibility among area suppliers. Many Quad Cities manufacturers interact with large customers like John Deere or Arconic, 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. Our community 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 local 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. There are over 1,200 local DoD suppliers; 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:

What are the biggest opportunity areas locally?
The Quad Cities Manufacturing Innovation Hub has identified three key opportunity areas in cybersecurity for area 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.

What are the business benefits of a cybersecurity program?
The business benefits of a cybersecurity program can be very impactful\(^2\)

- 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

---

2. Per Quad Cities Cybersecurity Alliance
Cyber-crime costs are predicted to hit $6 trillion annually by 2021. 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 local 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 Quad City universities and colleges. Turn to p.18 for a full list of area resources to jump start your cyber security journey.

---

# Table of Contents

How to Use This Playbook .................................................................................................................. 2
Whom can I contact at the Quad Cities Manufacturing Innovation Hub with questions? .................. 2
About the Quad Cities Manufacturing Innovation Hub and Our Partners ........................................ 2

Cybersecurity in the Quad Cities: At a Glance .................................................................................. 3
What does cybersecurity encompass? ................................................................................................. 3
Why does cybersecurity matter to the Quad Cities community? ....................................................... 3
What are the biggest opportunity areas locally? .................................................................................. 3
What are the business benefits of a cybersecurity program? ............................................................. 3
Where can I find help to get started? .................................................................................................. 4

Table of Contents ............................................................................................................................... 5

Understand the Technologies ............................................................................................................. 6
Additional Online Resources .............................................................................................................. 8

Identify Opportunities ....................................................................................................................... 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

Build the Business Case and Begin Implementation ........................................................................ 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 ............................................................................. 17
Metrics for Success: How to Measure Impact .................................................................................... 17

Find Help with Expert Partners ....................................................................................................... 18
Professional Organizations .................................................................................................................. 18
Consultants and Vendors ..................................................................................................................... 18
Hiring Solutions .................................................................................................................................. 19
Educational Institutions ....................................................................................................................... 19

Appendix ........................................................................................................................................... 20
Glossary: Cybersecurity Terms ........................................................................................................... 20
Understand the Technologies

In the first section, we take a closer look at the variety of technologies that contribute to the collective term “cybersecurity.” You’ll gain a better understanding of cybersecurity through diagrams, frameworks, and definitions of key terms. This section also details additional online resources for greater understanding.

We have defined cybersecurity as 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. Most of the information shared in this playbook will be on the process of identifying risks and designing secure systems and tools to mitigate those risks. We will use a couple of the most popular models as the basis for our common understanding.

The Large Organization
The breadth and depth of IT security systems can be quite complex. Large organizations will typically have a large security challenge driven by the complexity of their underlying information technology systems and networks. Regardless of the size of the organization, the risk analysis needs to be thorough. Every unaddressed vulnerability puts your organization at risk. While it is never possible to eliminate 100% of the risk, an organization can dramatically reduce the likelihood of an incident by anchoring their security programs to recognized security standards.

The good news is The National Institute for Standards and Technology (NIST) has a simple and logical framework to help you get started and prioritize and address the key risks (see Fig. 3).

Figure 3. The Five Functions of Cybersecurity

Executive Order 13636
On Feb. 12, 2013 the President issued an executive order that called for the “development of a “risk-based Cybersecurity Framework - a set of industry standards and best practices to help organizations manage cybersecurity risks.” The resulting Framework, created by NIST through collaboration between government and the private sector, will provide “prioritized, flexible, repeatable, performance based, and cost-effective approach” and enable organizations, regardless of size, degree of cybersecurity risk or sophistication, improve the security and resilience of their systems.5

The NIST Model
Figure 3 illustrates the high-level view of the cycle for managing an organization’s cybersecurity risk. This framework is the basis for most of the cybersecurity products and services being developed and provides a common language and framework to facilitate collaboration and communications across businesses and organizations.

Overview of the Framework
The framework is a risk-based approach to managing cybersecurity, meaning business drivers and activities help define the risk and the appropriate focus and mitigation strategies. The framework has three parts: framework core, implementation tiers, and framework profile.

The Framework Core
The core is organized around a set of five functions that describe the cycle for managing cybersecurity risk: identify, protect, detect, respond and recover. Each function is further divided into categories and subcategories. The core then describes the activities and desired outcomes, along with existing standards, guidelines, and best practices that apply to each category and subcategory.

Three Perspectives6

5 Ibid
6 Courtesy of Binto George, Ph.D., Professor, School of Computer Sciences, Western Illinois University
Cybersecurity threats can be viewed from three different perspectives namely, defense, offense, and use. First, defense is something that system administrators typically do to protect their systems from threats and the perspective most often taken. Second, to defend systems effectively we need to get into the minds of attackers and look at systems from the offense viewpoint. And finally, human factors make or break security, so it is critical to look at the security challenges from the use viewpoint. Your users can either help or hinder security, so it is important to design security that doesn't stand in the way of use. As you go through this playbook we would encourage you to take time to think about each issue from the additional perspective of the attackers and the users.

Glossary: Cybersecurity Terms
Please refer to the glossary in the appendix on p. 19 for definitions of key cybersecurity terminology utilized in this playbook.

Additional Online Resources
There are many online resources for review to deepen your understanding of cybersecurity strategies, programs, software, applications, technologies, use cases, opportunities, challenges, and more. We’ve outlined a few below:

- "Risk Appetite Statement" This whitepaper from Willis is not directly about cybersecurity, but it does a masterful job of describing why organizations need to be intentional as they deal with risk. Mitigating risk is what cybersecurity is all about and the fundamental insight on how to think about risk is a great place to start your journey. https://www.willis.com/subsites/australia/Documents/Publications/services/BusinessRisk/W0477_AU_Thought_Leadership_Article_Risk_Appetite_Statement_web.pdf
- “State of Illinois Cybersecurity Strategy” This document does a great job of describing the cybersecurity challenge, and how the state is addressing it. Any organization can learn more about what cybersecurity is, why it is important, and how to put a strategy together to meet the challenge. https://www2.illinois.gov/sites/doit/Strategy/Cybersecurity/Pages/cybersecurity.aspx
- IEEE Cybersecurity Initiative This website provides the go-to online presence for cybersecurity professionals with the goal to educate and improve cybersecurity program designs and implementations with current articles and case studies. https://cybersecurity.ieee.org/

Identify Opportunities
Cybersecurity offers many opportunities to small and medium businesses in the Quad Cities. The Hub has identified three key areas that can bring greatest benefit to our area’s small and medium manufacturers and the DoD supply chain.

Opportunity #1: Protect Your Company’s Data and Systems
Protecting your company’s data and systems begins with understanding the risks. Understanding and prioritizing the risks helps you adjust your procedures and training, as well as your investment in systems and tools. With a thorough understanding of the risks and a well thought out mitigation plan, the chances and potential severity of a breach can be greatly reduced protecting your company’s valuable assets and reputation.

Ibid
Opportunity #2: Minimize Impacts of an Incident
An organization can dramatically reduce damage through timely detection, preplanned response, and protected and backed up data. The time to think through your response and action plan is before an incident occurs. Proactive planning and thinking through possible corrective action scenarios buys you critical time and helps reduce the overall impact to the business.

Opportunity #3: Gain Competitive Advantage as a Secure Partner
The regulatory and commercial risk for large customers and DoD contractors is constantly increasing. Their business depends on your ability to meet the requirements of the DoD so they can meet their business commitments. Customers will award business to those they trust as being a secure partner; the risk is too great to do otherwise.

Benefits and Use Cases of Cybersecurity Opportunities
In this section, we’ll examine the key benefits of cybersecurity in each of the three opportunity areas previously identified.

Opportunity #1: Protect Your Company’s Data and Systems
- **Minimize disruptions of operations**: Eliminating opportunities for a breach reduces the risk of these common disruptions: machines and systems are down due to corrupted data, operating systems can become disabled or locked with a virus, the entire business may need to shut down until data is recovered and the root cause of the breach identified.
- **Reduce cost of recovery**: Proactively planning for an incident can reduce the time of recovery. The time saved from planning can be used to get into corrective action. Also, understanding your risks ahead of time dramatically increases your ability to accurately detect and mitigate the incident.
- **Protect your company’s brand and reputation**: Avoiding an incident is the best way to keep your reputation intact, but if a breach occurs, your ability to swiftly communicate and implement a corrective action plan can add to your reputation as a competent partner.

Opportunity #2: Minimize Impacts of an Incident
- **Reduce damage through timely detection and response**: Understanding your vulnerabilities is important to helping develop countermeasures, but it also enables you to establish early detection and corrective action plans. The damage that is done is often a result of your reaction time. Proactive planning and effective countermeasures can dramatically limit the damage.
- **Faster recovery times**: Time is money when it comes to response. By planning your recovery in advance of a breach, valuable time is saved. Understanding what is needed to recover is best done without the pressure of bringing a business back on line. A pre-established recovery process and communication plan can help you effectively restore your operations and your credibility.
- **Protected and backed up data**: Even with the best planning and reaction, a breach can result in a loss of data and contaminated programs. Having data and programs backed up and a system in place to convert to the backup is critical to restoring operations. Without it permanent damage to the business is likely.
Opportunity #3: Gain Competitive Advantage as a Secure Partner

- **Exceed customer expectations:** A solid cybersecurity program will impress your customers, but your ability to demonstrate that you are a secure partner by effectively dealing with a breach is “priceless.”
- **Reduce costs of non-compliance:** The best way to reduce cost is to eliminate incidents. The second-best way is to react quickly. Over time both will reduce your operating costs, making you more competitive in the marketplace.
- **Speak the industry standard language:** Being cyber-secure requires collaboration with the supply chain and the partners you choose to help you on your journey. Your ability to speak the language and interact in a knowledgeable and efficient way is another way to demonstrate that you are a secure partner.

Build the Business Case and Begin Implementation

In this section, we’ll outline the steps to implement a cybersecurity program within your company, beginning with awareness and change management, through establishing partnerships and building use cases that will save you time and money. We understand that the idea of implementing a cybersecurity program may be an entirely new technical area for your organization, and it involves everyone. We also understand that the prospect of this degree of change can be daunting! It is our hope that through the following content and previous look at the benefits of being cyber-secure you’ll feel more comfortable exploring how you can utilize these technologies to protect your data and systems.

Change Management: Building the Case Requires a “Test-and-Learn” Approach

For most small and medium manufacturers, the prospect of launching a cybersecurity program seems enormous, as it requires learning new technologies and procedures to prevent some future attack from an unknown enemy. The threat seems very hypothetical until you experience an incident. Only through thorough planning, continuous implementation, learning, and adjusting, can you build the expertise and experience that will keep your company’s assets safe for years to come.

These new digital technologies are shifting the supply chain into the next industrial age. Unfortunately, these new technologies depend on increased connectivity and the Internet of Things (IoT), dramatically increasing your exposure to cyber-crime. To be successful, you will need to pursue cybersecurity in ways that fit into your current culture, enrolling your people and aligning with your leadership’s risk management goals.

There are many ways for you to get started along the path to utilizing cybersecurity. Use the change management tips below to make the case for change and immediately begin proving results:

- **Create a vision of what success looks like and set goals accordingly.** Great metrics start with a clear vision of success. This vision will help identify the measures important to the organization. Metrics will include the business benefits along with project milestones that represent the progress being made in the implementation. Be sure to measure the initial progress and the quick wins that energize the organization. We have identified some typical metrics outlined on p.17.
- **Focus on getting every employee on board with the benefits of cybersecurity.** Get all stakeholders involved from the beginning via one-on-one conversations with leaders and all-company meetings to drive the vision. Make them as knowledgeable as you possibly can, taking ownership of cybersecurity. The IT professionals will be crucial in implementing the technical
solutions, but the success of a cybersecurity program relies on everyone following policies every single day. Turn to Quick Wins on pg. 17 for tips.

- **Plan thoroughly and implement continuously.** Initial planning should be large in scope to make sure all major risks are identified. After that, implementing a cybersecurity program is all about prioritizing and making choices. The typical company will have more risks than capacity to mitigate them, and risks and technologies change over time. Set the expectation that this is a never-ending journey but be sure to celebrate each milestone along the way.

Part of change management also lies in understanding and planning for the challenges you will encounter in integrating cybersecurity into your existing operations. Below are three challenges we’ve identified through our research and conversations with area manufacturers. Become familiar with the potential roadblocks so you can steer clear of their hindrances early on.

- **Challenge 1: You will never have enough resources.** The vast majority of the organizations implementing a program need help. Most companies have a limited budget for consultants, and consultants themselves are running at capacity. Part of the solution is to leverage internal resources where possible. Education and getting everyone involved is initially time-consuming but in the long run, a requirement.

- **Challenge 2: Your employees are not IT professionals.** Lots of education and patience will be required to train your employees the day to day skills required for success. Because the challenge is never-ending and technologies are changing quickly, education will need to be ongoing. In addition, the skills required for implementation and training may be outside your organization. Turn to Resources Needed: Technology and Staffing to learn more about hiring the right talent for the job.

- **Challenge 3: This feels overwhelming.** A thorough risk analysis is typically one of the first steps in implementing a program. The bad news is the analysis is likely to uncover a long list of required corrective actions and changes. The good news is the analysis helps prioritize which risks need immediate attention. Understanding risk and prioritizing is a key skill your leadership will need to wisely use your resources during the journey.

---

**Processes and Frameworks for Implementing Cybersecurity**

Integrating cybersecurity into your existing manufacturing processes requires a strategic approach. Utilize the workflows and frameworks on the following pages to aid in your high-level strategic prioritization of cybersecurity. We recommend you search out specific frameworks for each technology and use case chosen to guide your implementation.

**How to Get Started**

- Educate Leadership
- Assign Roles
- Take Inventory
- Find a Partner
- Create the Business Case
**Step 1: Educate your leadership.** There are many introductory training programs readily available regionally and virtually. These programs teach your organization the basic strategies to manage cyber risks. Each business typically has dozens of different risks and putting together a plan to deal with them is typically beyond the scope of these overview courses. However, you will find this very helpful if you are just beginning or upgrading your cybersecurity program. With this basic understanding in hand, you can better evaluate the resources needed to help in your journey.

**Step 2: Assign roles and responsibility.** Implementing or upgrading your cybersecurity program needs to be managed like any other investment your organization makes. Finding the person with the right skills to lead the project is critical. Basic understanding of the underlying systems and tools is important, but the project will impact every single person in your organization, so good people and communications skills are a must. Beyond the project management, leadership needs to support the project and take ownership of the activities in their functional areas.

**Step 3: Take inventory of your assets.** To scope and plan the project you need a basic understanding of what needs to be protected. A high-level map of your assets is a good way to start – anything that uses, stores, or transmits data: networks, devices, controllers, machines, computers, data storage etc. These can be stand-alone or connected, personal or company-owned, digital or paper-based. This will help leadership understand the breadth and depth of the risks involved.

**Step 4: Find a partner.** Most companies will need help. There are many resources, including from community colleges, accounting firms, IT consulting firms, and government funded organizations. Some regional choices are listed in our Appendix. If you approach the partner with a basic understanding of the cybersecurity process and your digital assets, you will have good chance of collaborating on a project proposal that meets your needs and budget.

**Step 5: Create the business case.** Avoiding the costs associated with an incident is the main reason organizations invest in the required countermeasures. There are numerous other business benefits of an effective cybersecurity program that are described in the following sections along with some guidance on how to calculate a return on investment (ROI).

**The Basic Business Benefits**
The business case for cybersecurity is based on cost-avoidance, which can be a challenging sell. Fortunately, business journals and media are packed with cybercrime stories making these risks real for every business. As more and more devices get connected to the internet, and more and more business is driven digitally, risks will continue to increase. Here are a few of the most frequently discussed reasons to be cyber-secure:

- Protects your business from costs of disruption to operations
- Protects your company’s brand and hard-earned reputation
- Avoids lost sales, penalties, and litigation expenses
- Small businesses or organizations are not immune; hackers target based on vulnerability.
- More and more companies are concerned about how their information is being stored/used.
- Most Federal agencies will require DoD/DFARS mandates.

**DFARS Certification**
Due to Executive Order 13556, contractors or sub-contractors to government agencies and organizations must provide documentation and evidence that they are protecting Controlled Unclassified Information
(CUI) to show DFARS compliance. To be considered in compliance, an organization must complete a security assessment based on National Institute of Standards Technology (NIST) Special Publication 800-171. In addition, any areas found to be at risk need documented remediation strategies. Contractors affected by this mandate must implement the remediation strategies in order to continue to do business with governmental agencies and organizations after December 2017. Those not in compliance may be fined or lose government contracts.

Calculating ROI
Calculating a return on investment (ROI) for your cybersecurity program can be a difficult task. Quantifying risk is the key to understanding potential return, and often the risks are not known until you are deep into the program. In addition, leaders seem to prefer projects that create traditional savings since they show up in increased profits. Cost avoidance is harder to appreciate since it focuses on keeping your costs from going up. Management understanding their appetite for risk is pivotal in guiding the organization’s investment.

\[
\text{Cost avoided} = \text{risk} - \text{cost of countermeasures}
\]

\[
\text{Risk} = \text{likelihood of an incident} \times \text{cost of the incident}
\]

\[
\text{ROI} = \frac{\text{cost avoided}}{\text{cost of countermeasures}}
\]

**Risk:** The product of the likelihood of exposure and the magnitude of the loss due to the exposure. The exposure is caused by criminals successfully exploiting vulnerabilities in business processes and systems. Cost of an incident can be based on experience or estimates gathered from industry studies, agencies, or consultants. Estimates will require lots of background and generally come under intense leadership scrutiny. The use of non-technical language and case study examples, along with your own internal assessment of risk helps make the numbers real.

**Cost of countermeasures:** The investment you make in resources and tools will be prioritized based on your risk. Your partner should be able to give you a good idea of the cost of each type of countermeasure.

If you are just starting a program, the one-time cost associated with consulting fees and staff time to organize and do an initial assessment is often taken out of the ROI analysis and considered part of the cost of doing business, especially if it is a government or customer requirement.

The following is an excellent article on calculating ROI:

Establishing or Improving a Cybersecurity Program
Once you are ready to begin, we highly recommend that you follow a proven methodology to thoroughly analyze your risk. Most consultants will use terminology and processes consistent with Section 3.2 of the NIST Framework and follow a process similar to the framework recommendations outlined below:

**Step 1: Prioritize and Scope.** The organization identifies its business/mission objectives and high-level organizational priorities. With this information, the organization makes strategic decisions regarding cybersecurity implementations and determines the scope of systems and assets that support the selected

---

business line or process. The Framework can be adapted to support the different business lines or processes within an organization, which may have different business needs and associated risk tolerance. Implementation Tiers may be used to express varying risk tolerances.

**Step 2: Orient.** Once the scope of the cybersecurity program has been determined for the business line or process, the organization identifies related systems and assets, regulatory requirements, and overall risk approach. The organization then consults sources to identify threats and vulnerabilities applicable to those systems and assets.

**Step 3: Create a Current Profile.** The organization develops a Current Profile by indicating which Category and Subcategory outcomes from the Framework Core are currently being achieved. If an outcome is partially achieved, noting this fact will help support subsequent steps.

**Step 4: Conduct a Risk Assessment.** This assessment could be guided by the organization’s overall risk management process or previous risk assessment activities. The organization analyzes the operational environment in order to discern the likelihood of a cybersecurity event and the impact that the event could have on the organization. It is important that organizations identify emerging risks and use cyber threat information from internal and external sources to gain a better understanding of the likelihood and impact of cybersecurity events.

**Step 5: Create a Target Profile.** The organization creates a Target Profile that focuses on the assessment of the Framework Categories and Subcategories describing the organization’s desired cybersecurity outcomes. Organizations may also develop their own additional Categories and Subcategories to account for unique organizational risks. The organization may also consider influences and requirements of external stakeholders such as sector entities, customers, and business partners when creating a Target Profile. When used in conjunction with an Implementation Tier, characteristics of the Tier level should be reflected in the desired cybersecurity outcomes.

**Step 6: Determine, Analyze, and Prioritize Gaps.** The organization compares the Current Profile and the Target Profile to determine gaps. Next, it creates a prioritized action plan to address those gaps - drawing upon mission drivers, a cost/benefit analysis, and risk understanding - to achieve the outcomes in the Target Profile. The organization then determines resources necessary to address the gaps. Using Profiles in this manner enables the organization to make informed decisions about cybersecurity activities, supports risk management, and enables the organization to perform cost-effective, targeted improvements.

**Step 7: Implement Action Plan.** The organization determines which actions to take in regard to the gaps, if any, identified in the previous step. It then monitors its current cybersecurity practices against the Target Profile. For further guidance, the Framework identifies example Informative References regarding the Categories and Subcategories, but organizations should determine which standards, guidelines, and practices, including those that are sector-specific, work best for their needs.

**Step 8: Continuous Improvement.** An organization may repeat the steps as needed to continuously assess and improve its cybersecurity. For instance, organizations may find that more frequent repetition of the orient step improves the quality of risk assessments. Furthermore, organizations may monitor progress through iterative updates to the Current Profile, subsequently comparing the Current Profile to the Target Profile. Organizations may also utilize this process to align their cybersecurity program with their desired Framework Implementation Tier.
Resources Needed: Technology and Staffing

Resources required to manage and implement a cybersecurity program will vary by the complexity of your systems and business. As was described in getting started, a basic inventory and map of your digital assets goes a long way in describing your future technology challenges and the skills required to address them.

A strong cybersecurity program will require an investment in internal and external resources: training, assessments, tools, consulting, and staffing. How and where you invest will be driven by your risk assessment and business needs. Clear priorities based on a rigorous risk assessment are the key to spending your resources wisely.

Hardware and Software: In implementing a cybersecurity program, hardware and software technologies go hand-in-hand.

Antivirus Software
The best antivirus software includes virus removal, internet security, malware and adware protection, as well as spyware removal. Viruses can make your computer run slow, steal important personal information or hold your computer ransom. Protecting against these types of threats typically requires you to download the antivirus software and pay an annual subscription charge. Most software will automatically update and scan individual devices to prevent or eliminate viruses.

Data Backup and Recovery
For most organizations, data is the lifeblood of their business. Data can get corrupted, infected, or lost. We have all heard stories of ransomware that cost companies many thousands of dollars to restore. To prevent this, your organization needs a process in place to periodically copy your data to a source outside your systems and retrieve it when and if needed. There are multiple approaches to data backup and recovery.

Some organizations or individuals use services, like Carbonite, to automate the process for their home or small businesses. Some homeowners or small business may prefer to do it themselves, manually connecting to an auxiliary storage device off their network and periodically saving data to that device.

Data backup and recovery for a larger business can be a complicated process. Where to back up the data is the first decision; cloud, on-site, or an off-site service are the main choices. Depending on the criticality of the data, frequency and security need to be considered as well. Weekly or daily backups may be good for some businesses where others may need real time updates so that no single transaction is lost. Some companies may need to encrypt and/or verify the security of the storage location.

Network and Vulnerability Scanners
Network scanning tools help discover all the devices present on your organization’s network. The discovery process provides details such as name, the type of device, and the operating system. Being aware of all the assets on your network is required if you want to defend your network from threats and attacks. Networks are often entered through devices that are overlooked in the analysis.

Vulnerability scanners are programs that include analysis routines that evaluate your network and devices looking for weaknesses. There are different levels of sophistication and commercial or open-source products designed to do these evaluations. Unfortunately, these tools are also used by hackers looking for vulnerabilities to exploit.
**Penetration Testing**
Penetration testing goes one step further than vulnerability scanning and tries to breach the system both from inside and outside the network. Testing includes network and application security as well as controls and processes around the networks and applications. Often, penetration testing may be a deliverable required to meet certain regulatory requirements.

**Firewalls and Intrusion Prevention Systems (IPS)**
Firewalls and IPS are security programs that monitor traffic coming into and out of your network. Data travels on the internet in packets, each with the data being transferred along with information about its origin. They use security protocols that look for and block suspicious data packet by packet coming into your network. There is subtle difference in the technology they use; firewalls and IPS are often found working in tandem to control incoming traffic.

Laptops should always run a software firewall to prevent unintended incoming traffic. Computer operating systems offer basic firewall security that can be supplemented with other commercial products based on your organization’s need.

**Employees and Hiring:** Assess your current employees for work habits, skillsets and experience in cybersecurity to determine if expertise and interest exists. If not, you may opt to hire new employees with cybersecurity expertise to speed up the implementation process. This article has some more detailed suggestions on work habits, soft skills, and technical foundation, both general and specific: https://insights.dice.com/cybersecurity-skills/2/

**Work Habits**¹⁰:
- Ability to work methodically and is very detail oriented
- Eagerness to dig into technical questions and examine them from all sides
- Enthusiastic and highly adaptable
- Strong analytical and diagnostic skills
- Demonstrated skills in innovation and collaboration
- Keep a current understanding of vulnerabilities from the Internet
- Maintaining awareness and knowledge of contemporary standards, practices, procedures and methods
- Ability to get the job done

**General Skillsets**¹¹
- Understand architecture, administration, and management of operating systems, networking, and virtualization software
- General programming/software development concepts and software analytical skills
- Proficiency in programming in Java, C/C++, disassemblers, and assembly language and programming knowledge of two or more scripting languages (PHP, Python, Perl, or shell)
- Understanding of how the different type of firewalls and network load balancers work
- Deep understanding of how network routers and switches work
- Evaluate and design systems and network architectures

Finding hiring partners will need to be a regional or national effort. Limited regional cybersecurity programs along with a very competitive market will make a local hire unlikely. Work with the education and hiring partners listed on p. 18 to find cybersecurity employees. Consultants are very actively

---

¹⁰ https://insights.dice.com/cybersecurity-skills/2/
¹¹ Ibid
substituting for internal capabilities as the cybersecurity talent shortage continues for the foreseeable future.

“Quick Wins” to Get Started with Cybersecurity
Take a page from the best practices of other manufacturers already up-and-running with cybersecurity programs by following a few of tips to jumpstart your use of these technologies.

- **Tip 1: Understand the scope of your challenge.** Taking inventory of your digital assets and mapping their integration is a good way to both educate your team and find some initial vulnerabilities. Prioritizing and executing some quick hits will give your team energy and maybe stop a potential threat. Addressing all your needs could take months or years. Having a solid plan based on prioritized needs makes the plan feel doable and practical.

- **Tip 2: Create organizational alignment.** Part of your challenge will be to change the culture. Changing culture is a complex task. For your employees to buy in, management must be clear on the importance of cybersecurity and how it is critical to the future of your business. Cybersecurity requires the implementation of new processes and behaviors throughout the organization. Make sure you take the time to involve your people in each step of the process creating their understanding and ownership.

- **Tip 3: Develop the needed resources and skills.** Most companies don’t have the resources and skills available to plan and implement a cybersecurity program. Many companies look at consultants to fill this gap. Make sure that you use the implementation phase as an opportunity to train your people. Also take the time to identify the level of skills needed in your company to sustain the program throughout your journey and hire and/or train the technical employees required.

- **Tip 4. Set the expectation that this is a journey.** Cybersecurity programs are based on the idea of continuous improvement. Cyber threats are constantly changing, and customer and government regulations increase over time. As your business changes, new risks will be introduced requiring new mitigation strategies. Tools and systems are being upgraded, making more effective solutions available to combat the evolving threats. This should always be thought of as a never-ending journey.

**Metrics for Success: How to Measure Impact**
When setting objectives for your cybersecurity program, you’ll need to use a combination of activity goals as well as business outcomes. The business benefits of avoidance are hard to quantify, but the activities need to reduce and mitigate risks are readily identified.

*Figure 5. Typical cybersecurity metrics*¹²:

¹² [http://securitymetrics.org/attachments/Metronic-6.5-Kwon.pdf](http://securitymetrics.org/attachments/Metronic-6.5-Kwon.pdf)
Find Help with Expert Partners

In delivering this Cybersecurity Playbook, among the seven other playbooks provided by the Quad Cities Manufacturing and Innovation Hub, our goal is to connect you to resources you need to learn about and implement new technologies that will impact your business and our region in the future. In this section, you’ll find experts, consultants, and specialists to help you succeed. This is only a partial list of the experts that can help you. We recommend researching partners based on your exact use case to narrow down the pool.

Professional Organizations
Quad Cities Cybersecurity Alliance
http://qccyber.com/
The Alliance brings together companies, NGOs, agencies, and municipalities for the purpose of raising awareness and providing education and awareness on cybersecurity issues and threats for the community. There is no cost to become a member, and it is a great place to meet organizations with similar challenges as well as IT professionals that can share insights and cybersecurity best practices.

Consultants and Vendors
Imprimis
http://imprimis-inc.com
Imprimis is a technology company out of Colorado that specializes in assessment and compliance tools. They have successfully worked with several Quad Cities companies as they begin their journey to become DFARS 800-171 compliant. Their tool set efficiently takes an organization through a self-discovery process that creates a cybersecurity program that meets government standards.
Procircular
https://www.procircular.com/contact/
Procircular is an Iowa-based consulting firm that specializes in cybersecurity. They offer a broad range of services from education and planning to implementation of individual tools to mitigate specific risks.

Twin State Technical Services
https://www.tsts.com/
Twin State Technical Services provides technology solutions to help businesses thrive, including infrastructure and network solutions to ensure a company’s network is operational and secure. Their security networkers ensure appropriate security measures are in place for their clients’ systems – from servers and websites to individual workstations and mobile devices. This includes any hardware, software, or human factors that may pose a security risk to your company. They also audit systems to test their strength, regardless of whether they had a hand in their development.

Heartland Science & Technology Group
https://www.heartlandstg.org/
Heartland Science and Technology Group is a 501(C)(3) not-for-profit corporation in Champaign, IL, founded by experienced engineers, researchers, and business professionals devoted to technical excellence and responsiveness to client needs. Heartland has developed a web-based cybersecurity dashboard demystifying challenging cybersecurity compliance processes and regulations set forth by the federal government. The Cyber Secure Dashboard tool (https://www.cybersecuredashboard.com/) provides the functionality required to implement, manage, track & communicate NIST cybersecurity requirements across the manufacturing enterprise, and maintain compliance through an evolving landscape of potential security threats.

Hiring Solutions
Robert Half Technology
https://www.roberthalf.com/technology
Robert Half Technology specializes in placing application development, systems integration, information security, infrastructure management, networking, database development, help desk and technical support professionals in project, contract-to-hire and full-time positions.

Chenhall Staffing Services
www.chenhallstaffing.com
In addition to staffing and HR, the Chenhall’s team provides solutions in a wide-ranging area of IT needs. Whether they are simply identifying and placing highly qualified technical experts to fit clients’ staffing needs or serving as a prime or sub-contractor on an operational program, their preferred operating model is to build long-term partnerships and trusted relationships with the common purpose of delivering, sustaining, and supporting quality IT services.

Educational Institutions
Western Illinois University (WIU) — Cyber Security, Bachelor of Science degree
http://www.wiu.edu/cbt/computer_science/cyber.php
The objective of the Cyber Security curriculum is to provide students with the theory, tools, technical expertise, and management know-how required to be successful in planning, designing, and managing a network environment.
Appendix

Glossary: Cybersecurity Terms

All definitions provided from the National Initiative for Cybersecurity Careers and Studies\textsuperscript{13} for educational purposes.

**Antivirus software**: A program that monitors a computer or network to detect or identify major types of malicious code and to prevent or contain malware incidents. Sometimes by removing or neutralizing the malicious code.

**Asset**: A person, structure, facility, information, and records, information technology systems and resources, material, process, relationships, or reputation that has value.

**Attack**: An attempt to gain unauthorized access to system services, resources, or information, or an attempt to compromise system integrity.

**Cybersecurity**: The activity or process, ability or capability, or state whereby information and communications systems and the information contained therein are protected from and/or defended against damage, unauthorized use or modification, or exploitation.

**Data breach**: The unauthorized movement or disclosure of sensitive information to a party, usually outside the organization, that is not authorized to have or see the information.

**Disruption**: An event which causes unplanned interruption in operations or functions for an unacceptable length of time.

**Enterprise risk management**: A comprehensive approach to risk management that engages people, processes, and systems across an organization to improve the quality of decision making for managing risks that may hinder an organization's ability to achieve its objectives.

**Event**: An observable occurrence that an incident is occurring or at least raise the suspicion that an incident may be occurring.

**Exposure**: The condition of being unprotected, thereby allowing access to information or access to capabilities that an attacker can use to enter a system or network.

**Incident**: An occurrence that actually or potentially results in adverse consequences to (adverse effects on) (poses a threat to) an information system or the information that the system processes, stores, or transmits and that may require a response action to mitigate the consequences.

**Incident response**: The activities that address the short-term, direct effects of an incident and may also support short-term recovery.

**Incident response plan**: A set of predetermined and documented procedures to detect and respond to a cyber incident.

**Intrusion**: An unauthorized act of bypassing the security mechanisms of a network or information system.

\textsuperscript{13} https://niccs.us-cert.gov/glossary
Mitigation: The application of one or more measures to reduce the likelihood of an unwanted occurrence and/or lessen its consequences by implementing appropriate risk-reduction controls based on risk management priorities and analysis of alternatives.

Preparedness: The activities to build, sustain, and improve readiness capabilities to prevent, protect against, respond to, and recover from natural or manmade incidents.

Recovery: The activities after an incident or event to restore essential services and operations in the short and medium term and fully restore all capabilities in the longer term.

Response: The activities that address the short-term, direct effects of an incident and may also support short-term recovery.

Risk: The potential for an unwanted or adverse outcome resulting from an incident, event, or occurrence, as determined by the likelihood that a particular threat will exploit a particular vulnerability, with the associated consequences.

Risk analysis: The systematic examination of the components and characteristics of risk.

Risk assessment: The product or process which collects information and assigns values to risks for the purpose of informing priorities, developing or comparing courses of action, and informing decision making.

Risk management: The process of identifying, analyzing, assessing, and communicating risk and accepting, avoiding, transferring or controlling it to an acceptable level considering associated costs and benefits of any actions taken.

Supply chain: A system of organizations, people, activities, information and resources, for creating and moving products including product components and/or services from suppliers through to their customers.

Threat: A circumstance or event that has or indicates the potential to exploit vulnerabilities and to adversely impact (create adverse consequences for) organizational operations, organizational assets (including information and information systems), individuals, other organizations, or society.

Virus: A computer program that can replicate itself, infect a computer without permission or knowledge of the user, and then spread or propagate to another computer.

Vulnerability: A characteristic or specific weakness that renders an organization or asset (such as information or an information system) open to exploitation by a given threat or susceptible to a given hazard.

Weakness: A shortcoming or imperfection in software code, design, architecture, or deployment that, under proper conditions, could become a vulnerability or contribute to the introduction of vulnerabilities.