Cybersecurity for Manufacturing

Manufacturers continue to face a wide range of concerns related to cyber security. It could be meeting the demands of the Department of Defense Cybersecurity Maturity Model Certification (CMMC) and other compliances, to the growing drive of Industry 4.0 and an increased emphasis on technology. This increase in technology reliance also has resulted in an increase of cyberattacks and threats to the production line.

This guide is designed to give a manufacturer the groundwork to build a security solution to help protect them from the dangers of one of the many different cyberattacks that could result in line production downtime and loss of revenue.

This whitepaper has four different sections that cover steps to protect manufacturers from cyberattacks, as well as how Encryption and Multi-Factor Authentication work, and why both are helpful in protecting a manufacturer's critical systems to keep the floor operating and products shipping out.

Table of Contents

NIST (National Institute of Standards and Technology)

The NIST Cybersecurity framework helps manufacturers to understand and manage cyber risk and reduce exposure. This framework provides best practices in implementing and designing your cybersecurity response. It helps you to outline and design your cyber response to protect your time, money, and provide you with a focus for your cybersecurity dollars.

6-Step NIST Cybersecurity Framework

1. IDENTIFY

Make a list of all equipment, software, and data you use, including laptops, smartphones, tablets, and point-of-sale devices.

Create and share a company cybersecurity policy that covers:

Roles and responsibilities for employees, vendors, and anyone else with access to sensitive data.

Steps to take to protect against an attack and limit the damage if one occurs.

2. PROTECT

Make a list of all equipment, software, and data you use, including laptops, smartphones, tablets, and point-of-sales devices.

- Control who logs on to your network and uses your computers and other devices.
- Use security software to protect data.
- Encrypt sensitive data, both at rest and in transit.
- Conduct regular backups of data.
- Update security software regularly, automating those updates if possible.
- Have formal policies for safely disposing of electronic files and old devices.
- Train everyone who uses your computers, devices, and network about cybersecurity. Help employees understand their personal risk, in addition to their crucial role in the workplace.

3. DETECT

Make a list of all equipment, software, and data you use, including laptops, smartphones, tablets and point-of-sales devices.

Monitor your computers for unauthorized personnel access, devices (like USB drives), and software.

Investigate any unusual activities on your network or by your staff

Check your network for unauthorized users or connections.

4. RESPOND

Have a plan for:

- Notifying customers, employees, and others whose data may be at risk.
- Keeping business operations up and running.
- Reporting the attack to law enforcement and other authorities.
- Investigating and containing an attack.
- Updating your cybersecurity policy and plan with lessons learned.
- Preparing for inadvertent events (like weather emergencies) that may put data at risk.

5. RECOVER

After an attack:

Repair and restore the equipment and parts of your network that were affected.

Keep employees and customers informed of your response and recovery activities.

6. REVIEW

It is very important to remember that any cybersecurity framework is not a one-time solution that you can “fire and forget.” Instead, it is a living document that should be reviewed on a regular basis (at least annually). As hackers and cyber criminals

continue to alter and expand their methods of attack, it is vital that small businesses remember to do the same. A security solution that has not been monitored and updated with the changing times risks being exposed and exploited.

If you would like to learn more about the framework solutions offered by On Technology Partners, please email us at info@ontechpartners.com with the subject **NIST Framework**.

Encryption Explained

Encryption, as it relates to a computer, is a method of protecting information by scrambling it up and making it unreadable without a special set of keys. This process is very similar to "writing in code" as a child. For example, the phrase "Hello There" using a 5-letter offset would become: "Cyggj Ocymy."

As you can see, the words become unreadable due to the shift in the lettering. In order to read the message, you need to know the rule that scrambled up the letters. This example also shows how encryption can be broken. For this simple encryption, it would be very easy for a person or program to quickly realize that the letters are off by 5 characters.

The more complex the encryption, the longer it takes for someone to find the patterns and decrypt it without permission. Fortunately, encryption is far more sophisticated and complex in protecting your data and information than that childhood code.

Because of this, you can think of your data being in two different states: encrypted and plain text. Encrypted means that a key is required to read it, and plain text means anyone can see it.

Two States of Data Encryption

There are two occurrences when it is very important to have your data encrypted:

1. **At Rest:** This is when your data is sitting on a hard drive, in cloud storage, or on a USB drive. When you think of data at rest, think about it in a saved place, but not being read or moved. Most of your data is at rest. Encrypting your hard drive or your smart phone is a way of protecting your data at rest.

2. **In Motion:** This is when your data is being transferred from your computer to another computer, and over the Internet. When you email or send a file over the Internet, in many cases, it is being transferred in plain text and is open to anyone. When a file is in motion, it is possible for a person it capture it as it moves along the Internet. This is why email is generally considered an unsecure environment. (The emails are in plain text when they are transferred between servers.)

When looking at encryption of your information, you want to confirm that your data is protected both at rest and in motion.

8 Things You Can do to Protect Your Information

Now that you know the basics, here are some practical steps you can take to protect your information:

1. If you are using a third party to back up your information, ask them if your data is encrypted on their servers and when your data is transferred to them.
2. Use a program, like BitLocker, to encrypt your computer. (There are similar Mac programs as well.)
3. Encrypt your USB and external hard drives.
4. Use a third-party system like Microsoft OneDrive to share files.
5. Use an email encryption program to encrypt vital emails.
6. Ensure that local backups use encryption.
7. Always verify that you are on a secure website before providing sensitive information. (You will see HTTPS instead of HTTP.)
8. Ensure that your website uses HTTPS encryption to protect your customers. (Notice how our site uses HTTPS to make sure that your information is secure.)

Are you wondering how you can implement encryption on to your email or computer? Reach out to us at info@ontechnology.com and ask us about our encryption solutions that help protect your team!

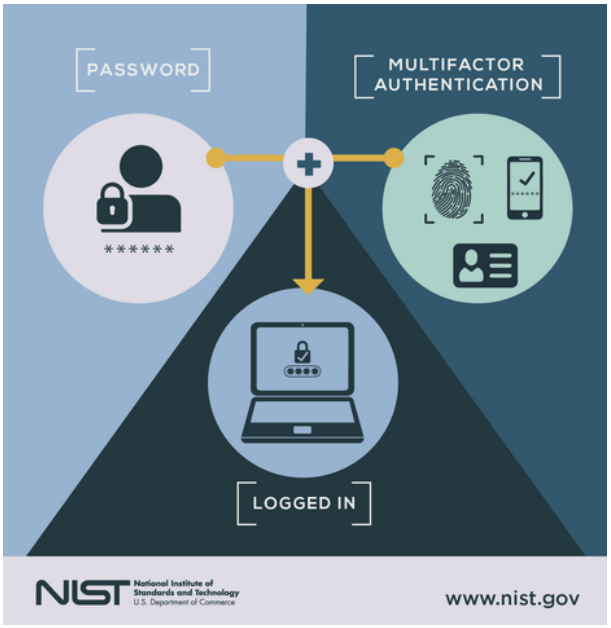
Multi-Factor Authentication (MFA)

Multi-Factor Authentication (MFA) is the process of having two or more authentication methods required for access to an account or service. Today, many of us already use Multi-Factor Authentication, sometimes also called 2-Factor Authentication (2FA), to access some of our accounts. For example: for many of us, our banks require us to type in a number or verification code that is texted to our cell phones, in addition to entering our password. By having multiple methods of authentication, it becomes more difficult for a hacker to take over your account. This is more difficult for hackers because they would not only need to gain access to your password, but would also need access to the secondary device, in this case, the cell phone being sent the verification code.

Here are some other examples of MFA that we use every day:

- Swiped your bank card at the ATM and then entered your PIN (personal ID number).
- Logged into a website that sent a numeric code to your phone, which you then entered to gain access to your account.

The chart below from NIST shows how MFA works to protect you:



Why Should You Care?

According NIST, 54% of all consumers use five or fewer passwords. This can create a domino effect that could allow hackers to access multiple accounts by breaking a few—or worse—a single password. If this occurs, a hacker could then gain access to your bank accounts, social media, email, sensitive files, and more.

By having MFA implemented, you reduce the ability of hackers to hack you and gain access to your vital data.

If you would like to learn more about how to implement MFA in your business, please contact us at info@ontechpartners.com with the subject **MFA.**

Making a Cybersecurity Master List

Why Make a List?

Your manufacturing business has many different assets that are vital to your operations. These items are the lifeblood of your company. Understanding what and where your assets are can make a major difference during (and following) a crisis or attack. It is also vital to know where your critical information is stored, who has access, and how to gain access to it. This document provides a summary list of possible items that you may wish to have as part of a cybersecurity framework.

Items to Include on Your Master List

1. **All hardware devices:** Having a list of all the company's physical assets is important in order to be able to respond to a loss or threat.

   This includes:

   - Laptops
   - Desktops
   - Printers
   - Network equipment
   - Smartphones
   - Tablets
   - Other technology devices

   Whenever possible, you should also capture the purchase data, serial number, and what the equipment was used for. This helps in the event that a device is lost or stolen.

2. **Software and cloud services:** Maintaining a current list of any legal software, cloud services (like QuickBooks Online, Carbonite backup, or Office 365) and storage services can be vital during a disaster. Being able to access cloud-based services is crucial if a device is lost or a location experiences a disaster and becomes inaccessible. Also remember to capture information about your website and social media accounts. We suggest having a password management service keep track of login and passwords for your company.

   Also remember to track all bank accounts and any passwords required to access them.

3. **Employee rights and access:** Employees may require different usage/permission rights to be able to perform their job. Knowing who has which rights is key to managing access to your vital information. Having a list of each employee with the level of access they should have is very helpful when an account is breached, or an employee decides to take undesired actions.

4. **Vendors and customers that have access to your system:** There are many vendors or customers that may need access to your internal information. For example, an accountant may need to access your QuickBooks, and a lawyer may need to review your documents. Knowing who your vendors are and what access they have could be vital in recovering after a disaster. If you have a third party managing your website, remember to keep all necessary web information as well. Loss of control of your company/business website could be devastating.

5. **Renewal dates and amounts:** Many vital business services are on a contract schedule. and knowing when items are coming due is vital to keeping services flowing. This is particularly true with services like domain registrations. Missing the renewal data on your company's domain could result in the loss of your ability to get email, have a web page, and contact your customers. If you need to transfer service for any reason, there may be a limited window in which to change. There could be major costs involved in missing that window.

Having vital manufacturing information in an easily accessible location could be the difference between being able to continue to run your business following an attack, or incurring thousands in costs to recover—or even worse—losing your business altogether.

*This information was gathered from FTC's website on small business cybersecurity.

If you would like to learn more about the asset management services offered by On Technology Partners, please email us at info@ontechpartners.com with the subject **Asset Management**.

Our **Free Manufacturing Cyber Risk Review** can help protect your team from hackers. To learn more, please visit: https://ontechnologypartners.com/manufacturing-cyber-risk-review-request/.

On Technology Partners
Partners In Productivity