# 4 Steps to Improved Cybersecurity

***By Eugene Jones, Senior Services Manager – Cybersecurity and Defense, Purdue Manufacturing Extension Partnership.***

Even though manufacturing is one of the top targets of cyber attacks, most small-to-medium manufacturers (SMMs) have not implemented basic cybersecurity controls. With 60% of small businesses failing within six (6) months of a breach, why aren't companies becoming protected? The answer is a combination of:

• Approximately 75% of manufacturing companies have fewer than 20 employees (score.org), and typically there is not a dedicated IT person. If there is an IT person, their time is consumed by system administrator duties, not network protection.

• SMMs don't realize they are a "target of opportunity," meaning the attack is aimed at any organization (opportunity) that is operating with a known operating system vulnerability. The hacker deploys malware that takes advantage of organizations with the known vulnerability. There are other reasons, such as a lack of information security awareness, or the perceived high cost of information security protections, but let's get to the steps to improved cybersecurity!

There are simple, low-to-no cost information security controls that can easily be implemented. Assuming you have an anti-virus application, start with these:

**1) Inventory.** You can't protect it if you don't know you have it! Once you know all of the software and hardware that is connected to your network, you can develop a system to keep those systems protected. There are tools that will inventory your applications and operating systems such as Lansweeper, which is free for up to 100 assets. The corollary to "taking" inventory is "controlling" inventory by limiting who can download software on your network, with local system administrative rights limited to a couple of people.

**2) Patch Management.** Once you have a solid inventory, you can implement a credible patch management routine. Patch management is routinely downloading the updates to ALL of your software and operating systems. While major applications such as MS Windows will download automatically, there are many that do not.

Let's pause. After the inventory, you know all of the assets on your network and using a routine patch management process, you keep these assets updated with the latest protection. Do these two things to reduce the risk of being a "target of opportunity."

**3) Train your Employees.** You don't need to train your employees to be cybersecurity professionals, but every employee needs to understand basic cybersecurity awareness. For example:

a) What types of emails should be viewed with skepticism and sent to IT for evaluation? (Risk of malware introduction.)

b) Why are certain websites such as social media and gaming sites blocked at work? (Risk of malware deployment.)

c) Why are portable media/flash drives used at work, but not permitted to be used on non-organizational assets at home or elsewhere? (Risk of introduction of malware from "lesser" protected systems.)

d) Why must each person on the shop floor have their own authentication for shared devices? (If malware is introduced, it gives the organization the ability to trace the incident back to a specific user.)

**4) Implement a Routine Back-Up Procedure.** Use the 3-2-1 Rule when it comes to backups. Create three (3) copies of your data – one primary backup and two copies. Save your backups to (2) two different types of media. Keep at least one (1) backup file off site.

**Conclusion.** The "4 Steps to Improved Cybersecurity" is not intended to be a complete list, but it is a good start. These actions will reduce the risk that your company is a target of opportunity for malware. If you are ready to do more, *Small Business Information Security: The Fundamentals (NISTIR 7621 Rev 1)* is a good free resource.