Georgia Tech | Georgia Manufacturing Extension Partnership
A unit of the Enterprise Innovation Institute

Cybersecurity for Manufacturing Companies

An Interview with Don Pital, GaMEP Growth Services Group Manager on… if, when, and how manufacturing companies should be concerned about cybersecurity.

On a scale of 1 to 10, how concerned are you about manufacturing cybersecurity?

Don: 10++. Cybersecurity is a ticking time bomb for most manufacturers. Many manufacturers are not concerned about protecting themselves or are only prepared with reactive tools, until they are hit with an attack on their system. For example, most would say they have passwords, firewalls, backups, etc. in place to protect them. These are good reactive steps, but there are many proactive steps that can be taken to keep you from having to use these! It's like having a home security system. Unless you test it, understand how it works, and then actually use it, you're relying on luck and possibly a baseball bat under the bed to keep you safe.

What are some preventative or proactive steps a manufacturer can take to prevent hacking or data theft?

Don: Well, I recommend following the National Institute of Standards and Technology's Cybersecurity Framework, including the most obvious step, which is to **Identify** who has access to your company information (using password control) and also to identify what equipment is on your network. A penetration scan by an IT service can show unauthorized devices. It is estimated by one cybersecurity firm that up to 20% of most networks contain undocumented devices (e.g. rogue printers, iPads, phones, etc.)

Isn't that just an employee training issue?

Don: It usually is. A company needs clear protection policies to limit who has access to the network and to secure network access points, particularly wireless ones. Other **Protect** and **Detect** steps that seem easy, but that are often routinely ignored are: updating anti-virus, anti-spyware, and other anti-malware programs and updating software and hardware operation patches. For example, when was the last time the Windows operating system that's running equipment on your plant floor was upgraded?

How is outdated software is a problem?

Don: It is a HUGE problem. For example, the Windows XP operating system came out 16 years ago and is still running in many plant operations. It isn't even patchable anymore as Microsoft no longer supports it. It can do a very good job running operations on a plant floor… until a vulnerability in the software is breached and then it's too late.

For more information on how GaMEP can help you create a cybersecurity plan, contact:

Don Pital, GaMEP Growth Services Group Manager
Georgia Manufacturing Extension Partnership (GaMEP) at Georgia Tech
Don.pital@innovate.gatech.edu
404-894-6117

Let's say a manufacturer has gone through the steps you recommend, but still gets attacked. What should they do then?

Don: It is critical that a company knows how to **Respond** and **Recover** from an attack. A manufacturer should have a response plan for cybersecurity incidents just like it has for emergency plant evacuation due to a fire or tornado. You should have answers to the questions:

- What do we do?
- Who is responsible for each step?
- What is the priority of response?

You mentioned the Recovery step. Can you elaborate?

Don: Having full backups of critical data when you need it most, is essential. Unfortunately, many manufacturers rarely test their backup capability or service to see if their data has been timely backed up and is readily available. Many manufacturers have an outside group backing up their data. This is a great step to ensure your data is up-to-date in case there is a breach, however make sure your data is truly being backed up by that company – as often and as laid out in your contract.

It has been estimated that up to 30% of attacked manufacturers go out of business within six months. So, again, a recovery plan is essential to a quick response and to prevent any loss of internal or customer data affecting your business. An attack may be inevitable, but your response and recovery plan will keep you in business.

It sounds like good cybersecurity is a must nowadays.

Don: It definitely is and continuing to ignore it puts manufacturers in great peril. My hope is that companies will take notice now and take the steps to prevent a disaster.

Find out more about the NIST Cybersecurity Framework and get started on or improve your plan to keep your company safe.

For more information on how GaMEP can help you create a cybersecurity plan, contact:

Don Pital, GaMEP Growth Services Group Manager
Georgia Manufacturing Extension Partnership (GaMEP) at Georgia Tech
Don.pital@innovate.gatech.edu
404-894-6117