5 Cyber-Security Tips for Small Business Manufacturing

Cyber-criminals have focused their sights on small business, with thousands of attacks occurring each day. The manufacturing sector is particularly vulnerable and now ranks second only to healthcare as the most targeted for cyber-attacks. Small business manufacturing organizations must be prepared or suffer the consequences.

According to Cisco's 2017 Midyear Cyber-Security Report, twenty-eight percent of manufacturers reported losing revenue due to cyber-attacks last year. Factory floor systems present unique vulnerabilities in protecting technical information. Increased automation and connectivity brings efficiency, but that improved performance comes with a price.

With so many systems connected via the internet, and with attacks increasing in sophistication, small business manufacturing should consider making cyber-security a top priority. Understanding both the opportunities and risks inherent in the Internet of Things (IoT) is critical to protecting valuable intellectual property.

Increased Connectivity and Risk

Exciting advances in technology offer greater efficiency and innovation to small business manufacturing. Workers monitor and adjust equipment from mobile devices. Vendors provide system fixes and updates remotely over the internet. Management can access comprehensive data analytics to adjust processes for maximum productivity.

However, the connectivity among machines and with vendors and contractors also brings inherent risks. Manufacturers often have no idea exactly what IoT devices connect through their networks.

In addition, technological advances mean that the lines have blurred between traditional informational technology and industrial devices. Interconnected systems often operate at differing levels of security with one system allowing more liberal access than another. Bringing together disparate systems opens up pathways for potential breaches.

Envision the damage an attacker could inflict by hacking the computer that controls a 3D printer or a robotic arm on the assembly line. Small adjustments to a design file or to the robot's configuration could result in downed production, costly recalls, or even danger to consumers.

Intellectual Property Theft

The digital transformation of manufacturing also increases the risk of industrial espionage. A recent study found that one in five manufacturers have lost intellectual property due to cyber-crime. According to the FBI, these thefts result in a yearly loss of approximately $400 billion.

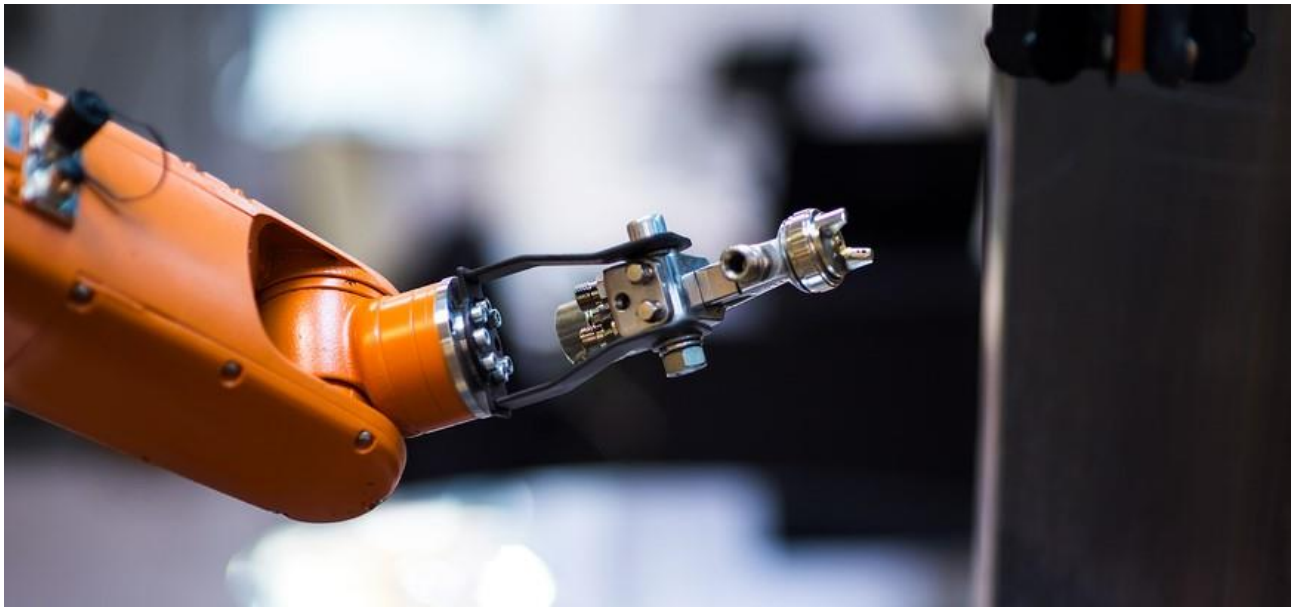
With so many interconnected systems, from the supply chain to connected machines, cyber criminals have multiple potential entry points. Once competitors gain access to product designs and trade secrets, they can quickly destroy an organization's competitive edge.

For many cyber criminals, social engineering provides the easiest path through an organization's defenses. Employees remain the weakest link in cyber defense.

Pro-active Defense for Small Business Manufacturing

Like pain management, cyber-security works best with a pro-active approach. Small business manufacturers that wait until a problem occurs may find the consequences of a breach too big to address effectively. Make cyber-security initiatives a priority, starting with a few key items.

1. **Know your network**—Make sure you are aware of what IoT devices are connected to your network. Apply updates and patches as soon as they are available.
2. **Conduct penetration testing**—Instead of simply patching vulnerabilities, conduct attack simulations to identify security weaknesses. Prepare for the worst case. Many manufacturers lack sufficient understanding of both current attacks and the limits of the security options available.
3. **Build a defense-in-depth security policy**—Work toward a layered defense policy that combines prevention with attack detection and response.
4. **Address the human element**—Make sure to document your cyber-security practices and train employees to use them. Also implement appropriate access control measures to ensure that users have only the access they need. This will help contain any potential breaches.
5. **Build more coordination between data operations and the factory floor**— Instead of informational technology (IT) and operational technology (OT) working in separate silos, both can benefit from shared data analysis and a combined approach toward cyber-security.



Simplifying Cyber-Security

For small business manufacturing, both the security risks and the solutions Increase in sophistication daily. According to the 2017 Cisco report, forty-six percent of manufacturers surveyed use at least six security providers. One in five manufacturers contract with more than ten vendors. This complexity presents its own problems.

To further compound the issue, many small business manufacturers lack sufficient resources to manage these risks. The current cyber-security workforce shortage and the complexity of the risks make effective cyber-security a challenge for many organizations.

Fortunately, the experts at managed security service providers (MSSP) make it their business to keep abreast of the ever-evolving cyber-security landscape. They provide technologies to detect and block attacks and design multi-layered proactive cyber defense solutions for manufacturers. Mitigate your risk with 24/7 network monitoring and a host of managed services solutions custom fit to your manufacturing business needs.