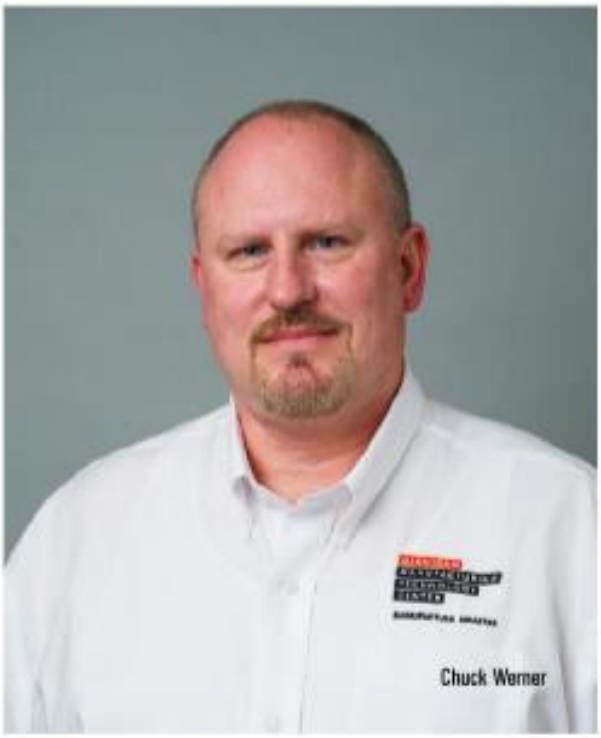
Applying Lean Manufacturing Principles to Information Security

By Chuck Werner, Lean Program Manager and
Jeff Williams, Program Manager, Cybersecurity,
Michigan Manufacturing Technology Center



Information, data and intellectual property may very well be among the most valuable assets to a manufacturer. But all too often, protecting these assets arn't given that level of priority in day-to-day operations. In a business environment where cyber threats are the new reality, manufacturers are increasingly at risk, with costly consequences. In fact, according to the FBI, $400 billion worth of intellectual property was stolen from U.S. businesses in 2017.

Manufacturers are particularly vulnerable/challenging position, as the U.S. Department of Homeland Security reports that manufacturing is in the top two target industry based on the number of reported cyber-attacks.

To protect proprietary information—and the future of their business, manufacturers can turn to a tried and true discipline: Lean Manufacturing.

Regarded as one of the most proven methods for lowering costs and reducing variation (through standardization), Lean uses a variety of tools to identify and reduce several types of waste, including:

Transportation
Inventory
Waiting
Defects

While these Lean principles are most often used to improve products and processes, they are not commonly applied to information security. To understand this connection, let's look at how lean concepts apply to the world of cyber.

Transportation

When products are unnecessarily moved in production, Lean defines this as transportation waste. In the world of information, data is often moved and copied to various locations. The downside to this practice is that more points of access to information also translates to more openings


Jeff Williams

for potential exposureas well as more effort required to keep that information secure. Consider the following questions related to transportation.

Are users allowed to copy data to removable storage (including laptops)?

Is more information shared to those in the production process than needed?

Inventory

Within the manufacturing environment, excess inventory often becomes obsolete and takes up unnecessary space. Worse yet, that inventory can confuse things and make it easier for mistakes to occur. The same holds true for the information we keep. Specific information may be needed to fulfill a contract or perform a task, but it is important to question if that information is critical for the business beyond completion, or simply information that a malicious actor could take advantage of. Much like removing excess inventory to optimize manufacturing processes, the best method to securing information is simply to not have it.

Waiting

Whether it's waiting for a machine to be ready, for the next individual to take over, or just for a decision to be made, manufacturing consists of much waiting. This can waste both time and energy. In the realm of data security, waiting can lead to the exposure of information. Is data "staged," waiting until it can be backed up or analyzed therefore exposing a location for exploitation? When sensitive data is printed, do employees wait to retrieve it from the printers, possibly allowing it to be viewed by others who shouldn't have access to it? In instances such as these, it is possible that waiting can derail a company's information safety.

Defects

Eliminating defects is a core focus of Lean, since mistakes in production result in costs and impacts to the business. Defects can be just as harmful in the world of information, such as with software patches and updates. While it may not be possible to completely prevent these defects from occurring, an organization can work to remove defects from their business environment. Consider the following questions:

> Eliminating defects is a core focus of Lean, since mistakes in production result in costs and impacts to the business

Is the organization's software still being analyzed and patched for security-related issues?

Are updates being applied as they are released to thwart potentially dangerous issues in information security?

Does the organization keep legacy software installed that is not being used, or it is removed when no longer needed?

Are users allowed to install unnecessary software as they wish?

Continuous Improvement

Outside of eliminating waste, Lean manufacturing also embraces the concept that all products and processes are not perfect and can be continuously improved. This way of thinking is also crucial to the protection of information. Threats are constantly changing. What may create a secure environment today may be insufficient to do so tomorrow. As more technology is incorporated into the organization, it is essential to continue analyzing business processes to make sure information remains adequately secure in the evolving cyber climate.

The Times, Theyare a-Changin'.

New technologies and evolutions in the world of information security will continually allow for the generation of new threats. But through diligence and an adherence to some simple Lean manufacturing concepts, it is possible toremain both protected and competitive.