5 questions manufacturing companies should be asking about their technology

We hear a lot about the convergence of IT and OT (operational technology) these days. Technology has long been a key part of manufacturing. However, factory automation and industrial control systems (ICS) have evolved on a separate path from information technology.

Tom Molden
CIO, Global Executive Engagement

Manufacturing and corporate technology domains have historically run independently. Different skill sets and different types of technology create a natural barrier between the two domains. Fear of operations disruption has led to moat-and-drawbridge approaches to protecting plants and a reluctance to make changes to the technology supporting the operating tools. Functional silos within IT and manufacturing have often led to tenuous relationships between manufacturing engineering and IT teams.

This has all changed over the past few years. Industry 4.0, connectivity to the internet, and the introduction of IOT and IIOT devices have changed the game. Manufacturing environments are increasingly connected to IT environments, and the technology domains are inextricably connected and interdependent. The good news is that the removal of barriers enables companies to operate more efficiently as well as mitigate risk more effectively.

As industrial companies think about modernizing their technology investments, they should ask themselves the following questions about their manufacturing estate:

1. Do I know everything that I have?

Everybody knows that you can't manage what you can't see; and in today's world, you can't protect it if you can't manage it.

In the legacy manufacturing world, asset inventory processes involved manual steps and were heavily dependent on spreadsheets. As more and more new asset types have been brought into the plant environment, many were not captured using these traditional scans. In worst-case scenarios, operators would simply unplug a device when it was time for a scan and plug it back in afterward. For years, outdated and incomplete information was accepted because it was more important to focus on things that keep the operation running.

Today's CIOs and heads of manufacturing understand the value of real-time visibility and a simplified, comprehensive view of assets across the corporate and manufacturing technology estates.

2. Am I managing and protecting my manufacturing estate holistically?

At a high level, there are two distinct types of technology in manufacturing. Industrial control systems are layered, as defined by the **Purdue model** and **ISA/IEC 62443 IACS Cybersecurity Standard**. From an asset management perspective, there is a principal distinction between device types and the expertise in managing them.

In the lower layers of the stack are devices that typically perform high-volume, repetitive work in the plant or industrial operation. Things like sensors and actuators must run with high degrees of efficiency and are intolerable of downtime. From a technology perspective, these devices generally run on real-time operating systems (RTOS), proprietary systems built and managed by ICS vendors. In recent years, OT security vendors have emerged that specialize in assessing and helping manage risk on these types of devices. In the Industry 4.0 era, we have also seen a proliferation of internet-connected (IOT/IIOT) devices brought into industrial environments, expanding the complexity to manage and the attack surface.

In the upper half of the stack are devices typically used to control the lower-tier devices, to provide overarching management functions, and to communicate with systems in the corporate domain. These types of devices usually run on standard operating systems like Windows and Linux and require the same type of management and control as systems in a corporate environment. There is also a layer of technology, sometimes referred to as "gateway devices," that manages the translation of protocols from the lower tier to the upper tier. Gateway devices often run on simplified, embedded versions of standard operating systems. All of these IT-like devices, and their connectivity to the corporate environments, represent the most common cyberattack vector and security exposure. In fact, for the first time in years, **manufacturing beat out financial services** as the most attacked industry.

To ensure they are managing and protecting their manufacturing environments end-to-end, manufacturing engineering, IT, and security teams are collaborating to form unified security operation centers (SOCs) and processes, pushing the best source of management data from these distinct types of technology into shared CMDB, SIEM, and workflow platforms.

3. Are my most critical assets patched?

Most IT and security practitioners would agree that the #1 way to protect against cyber threats is to keep your computers patched. Ensuring that you maintain the highest possible level of technology hygiene will also increase uptime and reduce the amount of effort you spend maintaining and fixing problems – like fewer trouble tickets so your help desk team can focus on more valuable work. The same rule applies in the manufacturing world: The IT-Like devices, or "managed assets" mentioned previously, all require similar levels and types of patching as assets in the corporate environment, and you should strive to carefully extend patching practices into the manufacturing space – ideally from the same platform that manages your IT assets.

History has shown that IT practices cannot be easily extended into manufacturing. Outdated operating systems, narrow change windows, thin hardware specs, and network segmentation are all traditional challenges to patching in the manufacturing environment.

However, with recent advances in technology and increased collaboration, manufacturing technology teams are increasingly able to improve operability and reduce risk without impact to production.

A note on vulnerability management: the process of identifying and prioritizing vulnerabilities helps you to focus your patching activity on the areas with the greatest risk. If you can drive your patching program from the same platform that you use to identify and prioritize vulnerabilities, you can eliminate hand-offs, get better results, and realize significant productivity improvements in your operations.

When it comes to the lower tier, or "unmanaged" assets, we are seeing more and more **cyberattack threats**. There are companies that specialize in identifying and analyzing vulnerabilities in this space, and best practices include aggregating data from those vendors' systems and your IT systems into a unified CMDB, SIEM, and workflow platform.

4. How well am I prepared for a cyber incident in manufacturing?

You don't have to go far to find advice on this topic. Given the recent surge of ransomware attacks, there are countless organizations offering best practices, solutions, and services.

First and foremost, you must have an incident response plan in place, and that plan must include manufacturing. It is important that your board of directors and other key executives know their roles. You should also have agreement on who has the ultimate accountability, and you should determine actions for as many scenarios as possible. For example, will you pay the ransom if attacked?

Can you recover from backups, and if so, how long does it take? If you've thought through the implications of many possible attacks, you will recover quicker. Test runs and tabletop exercises are great ways to ensure that all stakeholders are aware of the implications and prepared.

From a systems capability perspective, knowing the state of affairs is always critical during an incident. In an environment where minutes and seconds count, real-time visibility to what is going on in your environment is invaluable. A single source of truth is your friend, and the ability to take action and control assets from the same platform is also a big advantage in crunch time. The best-prepared companies know ahead of time where they are the most exposed and, in our resource-constrained world, can minimize impact by prioritizing the resources to remediate.

Then there's the cloud. Cloud adoption is growing across the manufacturing industry, and at the rate technology is advancing it is safe to assume that companies will continue to look for benefits from the scale and efficiency of cloud environments. Regardless of where you are on your cloud journey, it's a good idea to include cloud-based scenarios in your incident response planning.

5. What role is technology playing in optimizing my operational efficiency?

Is your reluctance to patch machines on the plant floor standing in the way of operational efficiency and increased manufacturing output?

Traditional manufacturing teams have a long-running aversion to touching anything that is running. Factory uptime drives output, and next to safety, output is the primary KPI for plant managers. Infrequent and short maintenance windows are normal, and an "if it ain't broke…." mentality is still prevalent in many places.

In today's world, however, the opposite is true. Industrial environments are full of machines that do work to manage the assets that are doing the physical work. Some of these require relatively little human interaction and are "out of sight, out of mind." There are also workstations and laptops used by factory employees that tend to receive less attention than in the corporate environment. In addition to the risk presented by these types of outdated, undermanaged assets, there is an impact on operating efficiency. Think about the number of resources spent "keeping an eye" on machines and then the implications when one of them eventually does go down or gets hacked. Add to this the resources you are employing to ensure that you comply with regulatory requirements. In addition to traditional compliance frameworks for industrial controls environments (e.g., ISA 62443), there are a host of more recent regulatory requirements around connected products that impact manufacturing (like UNECE R155/156 in automotive)

Now think about what this means at scale, with multiple factories or industrial operations running independently, each with its own set of resources managing their own set of outdated assets.

It is time to flip the script on managing manufacturing technology. In the traditional model, plants are managed independently: They operate in different parts of the world, in varying circumstances, with varying IT infrastructures. Add to these operations that have been added through acquisition. This model is inherently inefficient.

With the technology available today, and an embracing of good hygiene practices in the plant environment, companies can improve the standardization and centralization of operations. In addition to improving risk posture, this will have a positive effect on output.

In conclusion

The legacy of separate and independent manufacturing technology is inefficient and makes manufacturers ripe for cyberattacks. Outdated technologies are under scrutiny, a generation of manufacturing engineers is aging out of the workforce, and there are no good end-to-end solutions to manage and protect your assets.

The solution to these challenges begins with visibility. Start by unifying your IT and OT environments and draw confidence from always knowing what you have, where it is, and what state it's in. From there, the ability to control your assets from a single platform will help you eliminate hand-offs and manual processes.

Companies taking an end-to-end view of manufacturing technology and adopting an integrated platform approach are the most effectively managed and have the best-protected environments. The highest quality and most timely data from both IT and OT environments are feeding their SIEM, CMDB, and workflow platforms. They have a unified SOC and regulatory compliance is largely automated. Lastly, companies operating with efficiency as the end goal will gain a competitive advantage in the coming years.

Learn how the Tanium Converged Endpoint Management (XEM) platform can help manufacturers securly modernize their technology.

Contact us