The Complexities of Contemporary Manufacturing Will Require Assistance in Creating a Secure IT Infrastructure

By Chris West

According to the National Association of Manufacturers (NAM), a trade group dedicated to ensuring the success of the nearly 13 million men and women who manufacture things in the United States, in 2018 U.S. manufacturers accounted for 11.39% of the economy's total gross domestic product (GDP), or $2.3 trillion worth. That continued a decade-long upward trend in U.S. manufacturing output, rising steadily from $1.7 trillion in 2009, with the only annual dip experienced between 2015 and 2016, which saw a small decline from just more than $2.1 trillion to just less.

In other words, to paraphrase legendary Rock and Roll Hall of Famer Jerry Lee Lewis, on any given day at any given time, there's a "whole lotta *makin'* goin' on" in the U.S.

Truthfully, that has been the case since the first permanent settlements were established in what is now Virginia in the early 1600s, with the manufacturing industries ultimately becoming an important cornerstone in the foundational bedrock of the U.S. economy. Undoubtedly, the breadth of manufacturing in the U.S. has grown, expanded, modernized and evolved since the days when horse-drawn carriages, flintlock muskets and butter churns were the dominant in-demand items.

Over the ensuing 400 years, mind-bending advancements in the design and operation of manufacturing systems via the eventual development and use of computer-powered automation, monitoring, recording and safety technologies make modern-day manufacturing systems about as foreign to those from 50 years ago as they would be to the first colonial settlers. To say the least, gone are the days when an assembly line of workers performed specific repetitive tasks in order to produce a finished product, the total of which was tallied by a foreman standing at the end of the production line, clipboard in hand.

Today, every manufacturing process in every industry has evolved to the point where nearly all inefficiencies have been ironed out. This has led to the creation of streamlined manufacturing regimes that optimize design, engineering, labor and time costs, resulting in the construction of a finished product that can be made, depending on its complexity, in mere seconds, whether by human hands or robotics, or a combination of the two.

The Challenge

As mentioned, advances in computer-driven and controlled automation systems have been a boon to the manufacturing industry. They have also created an almost endless amount of performance-related data that can be studied and used to further improve any and all processes. The challenge then becomes, what is the best way for manufacturing companies to protect this data and keep it from prying eyes?

In the old days, an "uncrackable" safe was enough to keep unscrupulous people from stealing a company's "secret formula." Today, with so much proprietary production information gathered and aggregated within computer systems and then stored on the Cloud, the next attempt to access that sensitive information by nefarious people operating outside of the organization could be right around the corner.

External attempts to gain access to private and privileged manufacturing-system information generally take one of four forms:

- **Cybersecurity Threats:** Just like manufacturers are constantly working to develop new and better ways to make things, hackers, unfortunately, are always creating new ways of digging into data-storage systems that purport to be totally secure. The companies that work to build firewalls against this type of cyber invasion do a great job in foiling hackers, but you can never truly know when the next threat will rear its ugly head.
- **Data Overload:** The amount of operational and performance data that can be produced by an automated manufacturing system is mind-boggling. Knowing, first, how to securely store this data is vital, but getting your arms around the shear mass of it all and then using it in the best way to further improve performance requires a special set of skills. Many manufacturers do not have a person with this skill-set in-house, so they must reach outside the organization to secure the services of a partner that can aid in this area.
- **IT Infrastructure:** Too many manufacturers rely on legacy IT systems as the foundation for their operation and just cobble the newest software and hardware updates onto a frame that will one day not be able to support the weight of the entire system. It is also incredibly hard to maintain security within these Rube Goldbergesque systems, with outdated IT infrastructures generally having significant vulnerabilities.
- **The Digital Age:** As previously noted, when seen side-by-side, an assembly line from the 1970s would scarcely resemble one from today. Digital gathering of performance-related information is the "new normal" in most manufacturing processes. Maintaining these digital systems is a challenge within itself with, again, at the very least consultation from an outside source required in order to make the most of it.

The Solution

Knowing that their operations may be under constant assault, manufacturers need to collaborate with a partner that not only monitors, manages and maintains their automated systems, but also provides effective strategic guidance along the way. In other words, the best security partners deliver uptime and availability of all critical systems around the clock while also possessing the knowledge to assist in selecting and implementing both system upgrades or entirely new IT infrastructures, if needed.

Since 2003, Nexigen, Newport, KY, has been a leading developer of tools and services that can optimize operations and security protections for manufacturers who rely on automated production systems. Specifically, Nexigen offers Secure & Protect data, virus,

malware and phishing protections, Managed Services for desktop, network, server and WiFi, and Cloud Solutions platforms.

Specific to manufacturing systems, Nexigen offers the following services:

- **Network Security:** With any downtime – whether caused by equipment failure or a security breach – putting a damper on production schedules and product output, idled equipment can be a drain on the manufacturer's bottom line. Nexigen will work with the client to design, develop and execute a security strategy that will keep the risks of shutdown for any reason at bay.
- **Increased Visibility:** If something goes wrong during a production cycle, a stockpile of sensor-collected data concerning the operation of component parts, who supplied them and who built the machine, etc., will be the foundation for analyzing what caused the failure and making sure it doesn't happen again. Nexigen's system-monitoring capabilities enable it to analyze the situation and quickly isolate and identify other potentially affected production lines and runs, which will help get the system operational as quickly as possible.
- **Equipment Effectiveness:** An efficient, reliable automated manufacturing system requires the use of predictive-maintenance schedules in order to keep all components reliably operating at their best. Nexigen can track all usage patterns and maintenance data so that the operator will have a better idea when the specific piece of equipment may be due for its maintenance checkup, which will lower the risk that an untimely breakdown will occur.
- **Equipment Communication:** As new machines or components are introduced to the manufacturing system, they must be integrated into the corporate network. This means that some older machines will have to be retrofitted with the latest technology to meet newer standards and maintain their usefulness. Nexigen can build a communication network that will keep all components, no matter their age, tied together and communicating effectively, with no blind spots that can hamper production or compromise security.

Conclusion

Distilled down to its most basic form, manufacturing is still little more than a process requiring the insertion of Tab A into Slot B. It's the growth in the complexity of that process that has seen the manufacturing industry evolve from its early days into the highly efficient, fully automated process that is has become today. That increased complexity is found not only in the way things are done, but also in how performance data is collected, stored and utilized, and how it must be protected from unscrupulous actors. Recognizing the challenges that today's manufacturers – both internally from a performance and monitoring standpoint, and externally from a security standpoint – Nexigen has developed a complete suite of tools and services that can further codify and optimize "all that makin' goin' on."

About the Author:

Chris West is the Director of Sales and Marketing for Nexigen and can be reached at (859) 491-6601, ext. 257, or cwest@nexigen.com. Founded in 2003, Nexigen, Newport,

KY, is a developer and provider of Security, Managed Services and Cloud Solutions tools and systems that have been designed to optimize Internet Technology operations in the Manufacturing, Legal, Financial Services, Healthcare and Retail industries. For more information on Nexigen, please visit nexigen.com.