SOLUTION BRIEF

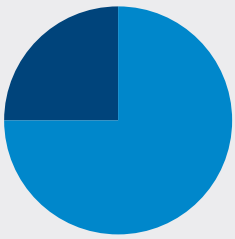
Achieve Smart Manufacturing While Protecting Intellectual Property

SecureWorks®

Introduction

Manufacturing is an important component in the global economy, contributing approximately 16 percent of worldwide GDP and about 14 percent of total employment.[1] Following a period of economic uncertainty, manufacturing is rebounding but with an increased emphasis on digital processes and technology. Global manufacturers are using advanced manufacturing technology to improve cost competitiveness, enhance processes and staff skills, and maintain connectivity with their all-important supplier ecosystem. Smart Manufacturing is using manufacturing intelligence and automation data to transform how products are invented, fabricated, shipped and sold as the physical and digital ecosystems meld to create new avenues and opportunities. However, the intellectual property and valuable data that underpins your manufacturing ecosystem also makes you a prime target for threats related to cyber espionage and cyber terrorism.

Manufacturing is the second most attacked industry after healthcare[3]



75%

of all private-sector R&D in the U.S. is for manufacturing.[2]

Manufacturing Industry Challenges

Manufacturing has experienced tremendous growth, with many firms embracing Smart Manufacturing and interconnected systems leveraging sensors and robotics to streamline operations, optimize costs and enhance competitiveness. Several challenges facing the manufacturing industry include accelerating time to market with new products, reducing costs and automating processes. The once labor intensive manufacturing industry has evolved to leverage automation where higher technology job skills dominate the value chain. Internet of Things (IoT) generates immense amounts of data across the shop floor, the supply chain and even via consumer utilization. There are over 20 million sensors globally today, monitoring and managing everything from raw materials to energy consumption to machine diagnosis and asset control. However, Internet connectivity of these devices makes them vulnerable to internal and external security attacks. According to *Dark Reading* magazine, manufacturing is the second most attacked industry after healthcare, making cyber espionage a real concern for your organization.[4] Maintaining uptime is essential where taking them offline to patch security gaps is less-than-ideal in a world of continuous production. Security frameworks and best practices must be a critical consideration as you develop and implement systems, not bolted on as an afterthought later.

Manufacturing Technology Brings Opportunity and Risk

Unlike other industries such as retail where hackers seek to monetize credit card data to sell on the black market, the manufacturing segment sees more threats centered on cyber espionage and cyber terrorism. Hackers that infiltrate a manufacturing platform or factory can modify processes or tools in order to make consumers ill or cause the manufacturing process to produce goods or tools that are out of alignment or even unsafe. According to the National Association of Manufacturers, manufacturers in the United States perform more than 75% of all private-sector research and development (R&D), driving more innovation than any other industry sector.[5] Many threat actors, who want intellectual property (IP) such as patent data, may also be from developing countries. Stealing IP can help them improve their manufacturing processes without investing substantial funds in R&D or to win bids and manufacturing sales proposals unfairly. Industrial control equipment can be an aging patchwork of vendors and equipment, none of it designed with security monitoring and management as a primary focus.

Top manufacturing industry challenges include:

- **Protecting Interconnected IT and Manufacturing Infrastructure:** Manufacturers operate with a level of trust between their manufacturing networks and their IT systems, creating a possible entry point for hackers seeking intellectual property like patents, proprietary processes and even costing and pricing for complex bids.
- **Securing Legacy Equipment:** Aging industrial control equipment was not designed with security in mind, and numerous gaps exist for hackers to exploit. Cyber attacks against industrial control systems (ICS) have increased in frequency and intensity as threat actors use evasive and persistent tactics to evade detection. More sophisticated malware attacks have been deployed on systems comprising U.S. critical infrastructure to compromise the system and reduce access in cases of cyber attack and "hacktivism".
- **Maintaining Equipment Uptime:** Factories often run 24x7 with around-the-clock production to optimize equipment and meet aggressive deadlines. Unlike IT systems that can be taken offline or patched at night, updating legacy manufacturing systems to remove common threats and vulnerabilities is a challenge.
- **Expanding Attack Surface with IoT Devices:** The extended ecosystem in Smart Manufacturing includes sensors and devices that monitor everything in real time, from raw inventory to processes to production metrics. The goal of Smart Manufacturing is to use this data to make better decisions and enhance speed to delivery, enabling organizations to take advantage of last-minute orders or changes in demand.
- **Enhancing Visibility with Continuous Monitoring:** Gone are the days when manufacturing and industrial control equipment ran in the background and off the radar screen of IT and security professionals — and threat actors. IoT has expanded the volume of data that you must watch and correlate for indicators of compromise and data removal or exfiltration. Increased monitoring and system-wide visibility is essential to ensure that no systems are breached; previous cyber threats have been found that went undetected for years that allowed threat actors to steal valuable IP and data like processes and formulas.

The factory of the future utilizes "always on" data such as inventory and production parameters that requires access to shop-floor systems and supply-chain partners. This merging of physical and digital ecosystems creates new optimization benefits and opportunities, as well as risks.

Conclusion

Smart Manufacturing is shifting industry dynamics towards technology-intensive processes and equipment with the goal of faster time to market and the next generation of mass customization. However, this speed and new technology focus brings both opportunity and challenges. Your evolving ecosystem that connects organizations, technology and devices to harness data for better decision making can also inject security gaps that threat actors can exploit. Legacy manufacturing systems and software were designed many years ago when security was not as top of mind, but protecting intellectual property should be paramount. You must think like a hacker and identify the intellectual property that cyber attackers want, and the myriad of methods to infiltrate your organization

and factory floor. Every second that a cyber attacker dwells in your organization increases the chance that valuable patents, processes and production output are compromised. Smart manufacturers with an eye towards smart protection understand that today's security is equal parts prevention and detection. SecureWorks helps manufacturers of all sizes develop and execute security frameworks that help you innovate and enhance your digital competitiveness.

SecureWorks provides an early warning system for evolving cyber threats, enabling you to prevent, detect, rapidly respond to and predict cyber attacks on your manufacturing operations.

SecureWorks Solutions

As a world leader in security solutions, SecureWorks provides an early warning system for evolving cyber threats, enabling you to prevent, detect, rapidly respond to and predict cyber attacks on your manufacturing operations. We deliver intelligence-driven security solutions and expertise in 59 countries around the world.

Security and Risk Consulting

Our Security and Risk Consulting team provides strategic advice and analysis to help you enhance your manufacturing security posture, reduce your risk, facilitate compliance and improve operational efficiency. Our highly skilled security consultants help you test and improve your security defenses, design security processes and develop new security programs. SecureWorks offers IoT consulting and assessment services for worldwide manufacturers large and small.

Managed Security Solutions

SecureWorks offers a wide range of managed IT security solutions for manufacturing organizations. The Counter Threat Platform™ is at the core of our intelligence-driven approach to security solutions. The CTP analyzes billions of network events 24x7 to discover potential threats, deliver countermeasures, and generate valuable context and threat insights for all industries including the manufacturing industry. We help you detect advanced persistent threats (APTs) and mitigate any damage they may have caused.

Our security analysts serve as an extension of your team to monitor for, and detect, threats across your environment. For manufacturers, we provide management and monitoring that can identify true threats and eliminate false positives that can distract your time and attention.

Threat Intelligence

The SecureWorks Counter Threat Unit™ research team collects relevant information wherever it can be found, and then analyzes it and synthesizes it into meaningful guidance on which you can act. Our threat intelligence helps you identify threat actors who may be specifically targeting your organization or executives, and provides the insights to help you defend and even preempt the attacker.

Incident Response and Management

Our incident management practices provide rapid containment and eradication of threats, minimizing the duration and impact of a security breach to your manufacturing organization.

Leveraging our cyber threat intelligence and global visibility, we can help you prepare for, respond to and recover from even the most complex and large-scale security incidents. SecureWorks has the people, processes and technology to help you detect threats sooner to minimize damage and identify root causes to avoid becoming recompromised.

For more information, call **(877) 838-7947** to speak to a SecureWorks security specialist.

www.secureworks.com

End Notes

[1]McKinsey&Company, "Manufacturing the future: The next era of global growth and innovation", http://www.mckinsey.com/business-functions/operations/our-insights/the-future-of-manufacturing, accessed August 28, 2016.

[2]National Association of Manufacturers, "Top 20 facts about manufacturing", http://www.nam.org/Newsroom/Top-20-Facts-About-Manufacturing/, "Manufacturers Suffer Increase In Cyberattacks " accessed August 16, 2016, accessed August 25, 2016.

[3]Yasin, Rutrell, *Dark Reading.com,* http://www.darkreading.com/vulnerabilities---threats/manufacturers-suffer-increase-in-cyberattacks/d/d-id/1325209, accessed August 20, 2016.

[4]Ibid.

[5]National Association of Manufacturers, "Top 20 facts about manufacturing", http://www.nam.org/Newsroom/Top-20-Facts-About-Manufacturing/, accessed August 16, 2016.