A Forrester Consulting
Thought Leadership Spotlight
Commissioned By Armis

September 2019

State Of Enterprise IoT Security: A Spotlight On Manufacturing

Manufacturing Industry Results From The September 2019 Thought Leadership Paper, “State Of Enterprise IoT Security In North America: Unmanaged And Unsecured”

FORRESTER®

Introduction

Faced with lower-cost competition and ever-increasing customer expectations, manufacturing firms are turning to technology to both help them operate more efficiently and to differentiate themselves in the market.[5] Industry 4.0 has seen the introduction of digital technologies, including millions of unmanaged and internet of things (IoT) devices. The large number and great diversity of IoT devices has increased the attack surface and created new security exposures for manufacturers.

In July 2019, Armis commissioned Forrester Consulting to evaluate the current state of IoT security in North America. To explore this topic, Forrester conducted an online survey of 403 technology decision makers responsible for IoT security in their organizations. The research also included three interviews with CISOs and IT project managers across various industries. This spotlight focuses on the results of the 100 survey respondents and one interviewee from the manufacturing industry.

KEY FINDINGS

- **The use of unmanaged and IoT devices in the manufacturing industry is prevalent and growing rapidly.** Ninety-one percent of respondents have seen an increase in these devices in the last 24 months, and half of the respondents report that the use of these devices has increased by more than 50% over the same period of time. The increase has occurred everywhere — from the shop floor to the executive suite. Sixty-six percent of professionals in the manufacturing industry attribute the increase in usage to internal factors such as digital transformation strategies. Many of our respondents are very-to-extremely concerned about external hackers (84%), as well as viruses, network worms, and other malware threats (80%).
- **Complexity and convergence result in security incidents.** Manufacturing professionals feel more confident in their ability overall to protect unmanaged and IoT devices than other industries do; 56% of respondents say they fully understand the risks associated with unmanaged and IoT devices. However, the majority also believes that their devices are safe behind a firewall (75%), despite the recent publicity concerning attacks against manufacturing and industrial firms involving malware that was not blocked by firewalls - including WannaCry[1], NotPetya[2], Triton[3], and LockerGoga[4]. In fact, attacks on unmanaged or IoT industrial devices are real and frequent, with 66% of the respondents saying they have experienced a security incident, a result similar to the average of all respondents in our survey (67%).
- **Investment in IoT security solutions is insufficient and needs to increase.** The top priorities of security professionals in the manufacturing sector are to improve visibility on unmanaged devices connected to the network (51%) and to deploy agentless security solutions (48%).

76% of manufacturing enterprise IoT professionals feel their current security controls and practices are not adequate for unmanaged and IoT devices.

"Our plant equipment is usually built on older operating systems that are often forgotten, and therefore, not subject to the usual patching and vulnerability management cycles […]. This leaves a big gap from an attacker perspective."

CISO, global food manufacturer

DEFINING AN UNMANAGED OR IOT DEVICE

For this study, we defined unmanaged and IoT devices as any system that can communicate with other devices and systems in your organization, process and transmit information, has an operating system (no matter how simple), but cannot be managed via traditional security tools. Such devices can include, but are not limited to:

Industry-specific devices	Industrial control systems (PLCs, HMIs, robotic arms, etc.), medical devices (patient monitoring systems, mobile imaging systems, infusion pumps, communication badges, etc.), retail (barcode scanners, POS system, loss prevention, etc.), warehouse (inventory systems).
Office devices and peripherals	Printers, VoIP phones, smart TV screens and monitors, Bluetooth keyboards, headsets, etc.
Building automation	HVAC systems, security systems, lighting systems, cameras, vending machines, etc.
Personal or consumer devices	Smartphone, smart watch, gaming consoles, Apple TV, Slingbox, digital assistants (Amazon Echo, Google Home, etc.), cars.
IT infrastructure	Access points, routers, switches, firewalls, baseboard management controllers of servers.

66% of manufacturing firms have experienced an IoT-related security incident.

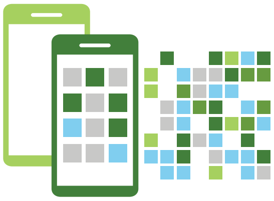
Digital Transformation Initiatives Fuel The Growth Of Unmanaged And IoT Devices

As sensor technology and automation systems become more embedded in plant equipment, the digital transformation of traditional manufacturers is characterized by the convergence of IT and operational technology (OT). In surveying 100 enterprise security professionals in the manufacturing industry (see Appendix B), we found that:

- **Ninety-one percent have seen an increase in the use of unmanaged and IoT devices in the last 24 months.** As a result, the enterprise IoT environment now makes up a significant portion of the larger IT ecosystem: 73% of surveyed organizations estimate that at least half of all devices on their enterprise network are unmanaged or IoT. To complicate matters, changes in the IoT environment have been happening at a higher speed than in other industries; 54% have seen a greater than 15% increase in the number of IoT devices in just the last two years.
- **The growth of unmanaged and IoT devices comes mainly from business-driven initiatives.** With the aim of reducing costs and improving operational efficiencies and regulatory compliance, manufacturing organizations have been introducing IoT devices to all areas of their operations, as evidenced by the convergence of IT and OT. This study found that these business initiatives play the largest role in driving the growth of IoT in manufacturing, with 66% of respondents agreeing that "our company is pursuing digital transformation strategies to improve core business processes, and this transformation requires IoT devices."
- **Unintended introduction of unmanaged or IoT devices is also significant.** While not as large as the growth in devices from business initiatives, manufacturing had a larger growth of devices than any other sectors of these devices due to employee or other sources. Forty-seven percent of respondents from the manufacturing industry — larger than in any other segment — stated that employees are bringing connected devices with them into the office environment, and 54% stated that device manufacturers are constantly building connectivity into everything, whether they want it or not.
- **Manufacturing security professionals are concerned with risk exposure.** Attacks on unmanaged or IoT devices can lead to downtime, disruption to business operations, and even environmental risks, which can significantly cost manufacturers. Seventy-four percent of manufacturers reported feeling very-to-extremely concerned about the security risks posed by unmanaged and IoT devices, and 78% believe that unmanaged and IoT devices are more vulnerable to cyberattacks than corporate-managed computers. The main concerns of other industries are the loss of sensitive data, whereas manufacturing respondents are more concerned by external hackers (84% of them being very-to-extremely) and viruses, network worms, and other malicious software (malware) threats (80%).

While unmanaged and IoT devices bring the promise of boosting the understanding of how well manufacturing environments perform, they offer little in the form of security, creating new security exposures for organizations.

91% of respondents have seen an increase in the use of unmanaged and IoT devices over the last 24 months.



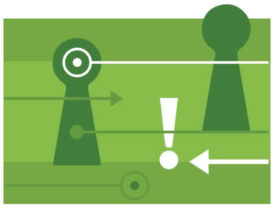
> "If these devices have not properly been discovered and therefore managed and monitored, it will be difficult for us to protect our company in the long run."
>
> *CISO, global food manufacturer*

Complexity and convergence result in security incidents.

Unmanaged and IoT devices introduce various and different security risks into organizations, but many IT managers admit that they are not fully aware of these risks, nor are they equipped with the knowledge, skills, and resources to sufficiently manage them. As a result, enterprise security professionals fail to address the security threats brought on by unmanaged and IoT devices:

- **Most enterprise security professionals profess confidence in their ability to protect unmanaged and IoT devices connecting to their network. . .** Professionals from the manufacturing industry feel more confident overall in their ability to protect unmanaged and IoT devices than other industries do.
- **. . . But further study revealed some gaps.** Security frameworks (e.g., NIST and CIS) are not universally applied, with 30% of manufacturing respondents not following them.[6] The complexity of their IT environment, coupled with a lack of know-how (75% think that unmanaged and IoT devices are safe behind their firewall), makes it even more difficult to buy and implement solutions that would effectively secure all their devices. As a result, the industry is regularly targeted by attacks.[7] With some of these attacks causing the physical destruction of equipment.[8] IoT-related security incidents are as frequent in manufacturing as they are than in other industries, with 66% of the respondents saying they have encountered an incident.
- **As a result, most organizations fail to secure unmanaged and IoT devices, and thereby suffer from the consequences of security incidents.** Consequences from security breaches have affected manufacturing companies in multiple ways, including data leakage in 70% of the cases, raised customer data privacy concerns for 56% of the organizations, and reduced revenue for 45% of them. Other concerns that are higher in the manufacturing sector than other sectors include safety issues (27%) and legal and regulatory costs (26%) (see Figure 1).

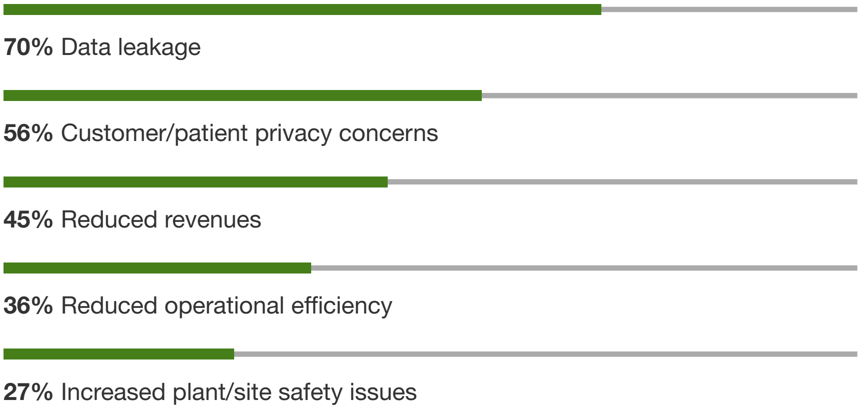
As they modernize their OT, the extent of security exposure for unmanaged and IoT devices is often not well understood or addressed by enterprise security managers in the manufacturing industry. Security incidents are now forcing them to look at how to better mitigate those risks.



66% of manufacturing organizations surveyed have experienced a security incident related to unmanaged or IoT devices.

Figure 1

“What consequences has your organization experienced due to security incident(s) associated with unmanaged or IoT devices?” (Showing Top 5 only.)



Base: 100 technology decision makers with responsibility over IoT security at US and Canada manufacturing firms
Source: A commissioned study conducted by Forrester Consulting on behalf of Armis, July 2019.

Investment In IoT Security Solutions And Practices Must Increase

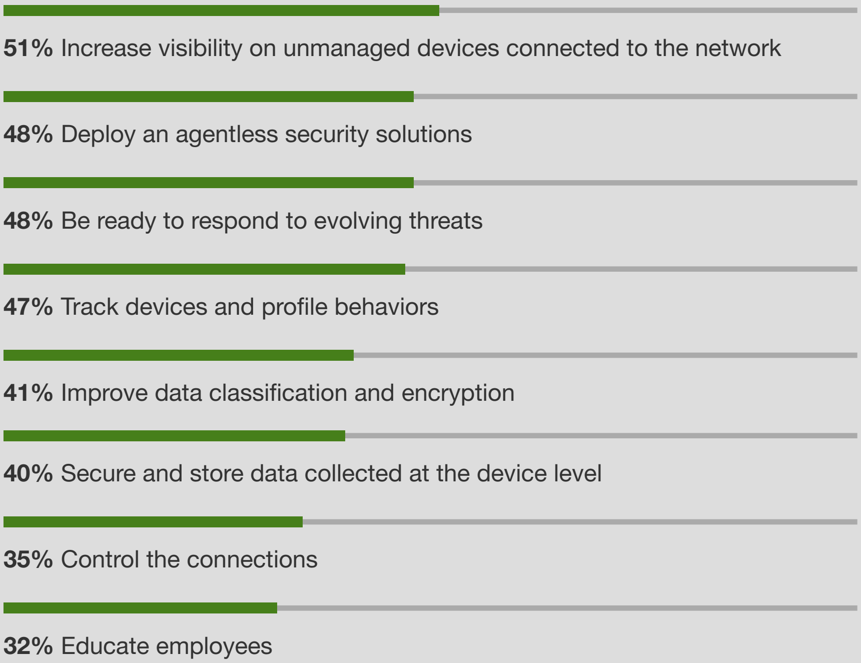
Manufacturers must be prepared to address the additional security exposures and vulnerabilities related to unmanaged and IoT devices. As suggested by security frameworks from organizations such as NIST and CIS a broad spectrum of security functions are required to properly secure unmanaged and IoT devices. In response, we found that enterprises are planning to increase spending on IoT security and to deploy a broad range of controls.

96% of respondents plan to increase their budget dedicated to unmanaged and IoT devices security in the next 24 months.

- **To respond to increasing risks, budgets dedicated to unmanaged and IoT devices security must increase.** As organizations come to realize the extent of IoT security risks, either through their own experience and as more breaches become publicized, they will rationalize the need to allocate more resources to securing their unmanaged and IoT devices. Ninety-six percent of enterprise security professionals from the manufacturing industry say they will increase their security spending dedicated to those devices over the next 24 months. About half of them (46%) plan to increase their spending significantly by 10% or more.
- **In alignment with popular security frameworks, a broad spectrum of security functions will be deployed.** The top priority of enterprise security professionals in the manufacturing industry is to direct their IoT security spending toward improving visibility on unmanaged devices connected to their network (51%), and deploying an agentless solution (48%), since agents can’t be used to monitor or protect unmanaged or IoT devices (see Figure 2). Visibility is a key aspect for this industry, with 100% of the respondents saying they already use, or plan to implement in the next 12 months, security controls and practices supporting device visibility (see Figure 3). Organizations will be looking to partner with solution providers that help them overcome their main challenges, e.g., navigating the complexity of their IT environment (62%) and being ready to respond to the changing/evolving nature of internal and external IT threats (46%).

Figure 2

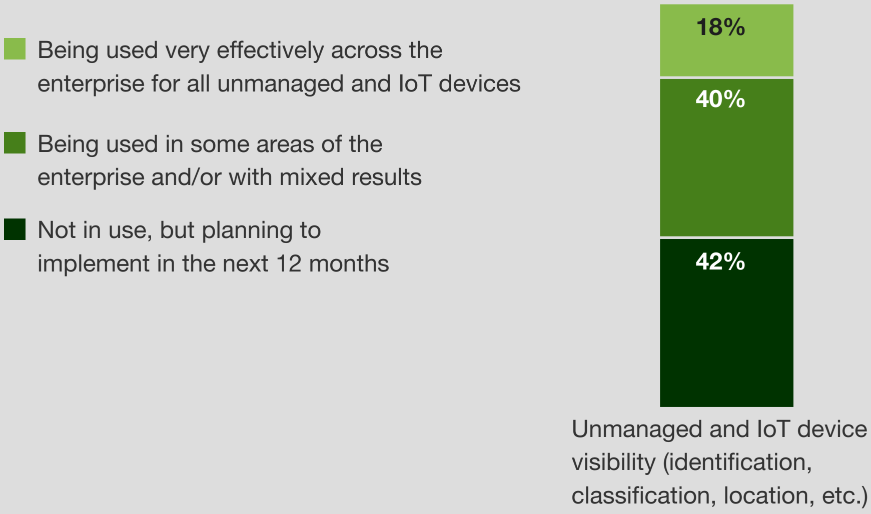
“What are your organization’s top priorities when it comes to IoT security for the next 12 months?”



Base: 100 technology decision makers with responsibility over IoT security at US and Canada manufacturing firms
Source: A commissioned study conducted by Forrester Consulting on behalf of Armis, July 2019

Figure 3

“Which of the following security controls and practices are being used for unmanaged and IoT devices throughout your enterprise, and how effective is each?”



Base: 100 technology decision makers with responsibility over IoT security at US and Canada manufacturing firms
Source: A commissioned study conducted by Forrester Consulting on behalf of Armis, July 2019

Key Recommendations

As the use of unmanaged and IoT in manufacturing environments continues to grow, so does the importance of implementing security solutions, practices, and controls that can identify and protect these devices. While manufacturers are excited about the efficiencies and insights they can gain from deploying IoT-enabled equipment, improper and inadequate security controls put organizations and customers at risk of downtime, data loss, costly remediations, etc. Furthermore, any downtime caused by cyberattacks creates real impact — from lost revenue for not delivering orders on time, to negative customer experiences and supply chain disruptions. These threats demand an aggressive and comprehensive cybersecurity posture to defend against the myriad of new threats that unmanaged and IoT devices introduce. Without such security protections, organizations are vulnerable to cyberattacks and their potentially long-lasting effects.

Forrester's in-depth survey and interviews of enterprise security professionals about unmanaged and IoT devices yielded several important recommendations:

Assess and inventory your enterprise and industrial IoT devices. You cannot secure things if you don't know they exist. This demands completing a thorough inventory of all devices connected to your network — everywhere, from the shop floor to the executive suite — and then using that information to build policies and implement controls to ensure devices are appropriately monitored and secured. Doing so will minimize the risk of unintended data breaches or other related security incidents.

Prioritize device classification and protection, and use it to build the appropriate controls. Leverage the inventory of devices to understand how and where they are used, how they drive the business, what critical data they have or activities they perform, and how they may be exploited or manipulated. This will help ensure your security policies are effectively applied, and security frameworks, such as NIST and CIS, properly enforced for unmanaged and IoT devices in all areas of your enterprise — from the assembly line to the back office.

Raise awareness on growing unmanaged and IoT device security risks. As an enterprise security professional, you need to demonstrate to decision makers in your organizations that unmanaged devices are more vulnerable than managed computers and, at the same time, are not as well protected as managed computers, since they can't accommodate standard security agents and be easily patched. This will help you build the business case to secure additional budget allocation to acquire the necessary technologies and resources needed to properly secure unmanaged and IoT devices and mitigate risk to the business.

Anticipate future threats by implementing solution(s) that provide device visibility, risk assessment, threat detection, and other protections specific to unmanaged and IoT devices. As security professionals identify their needs, they should create a comprehensive IoT security architecture that addresses their organization's specific IoT use cases and security requirements. The challenge here is that many security solutions were built for traditional computers and don't work for unmanaged and IoT devices. New, purpose-built solutions are now available in the marketplace, and should be carefully looked at. However, ensure those solutions address the strategic security need, deliver the appropriate security measures for the devices in question, and integrate with existing security and management tools.

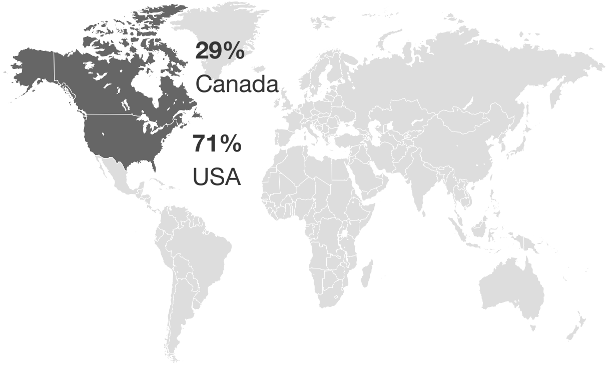
Appendix A: Methodology

This spotlight is based on a wider Thought Leadership study that looked at the state of IoT security at North American enterprises. In the original study, Forrester conducted an online survey of 403 technology decision makers responsible for IoT security in their organizations, and three interviews with CISOs and IT project managers across various industries. Questions provided to the participants asked about their challenges and priorities, budgets and planning, and use of unmanaged and IoT devices security solutions. The study was conducted in July 2019.

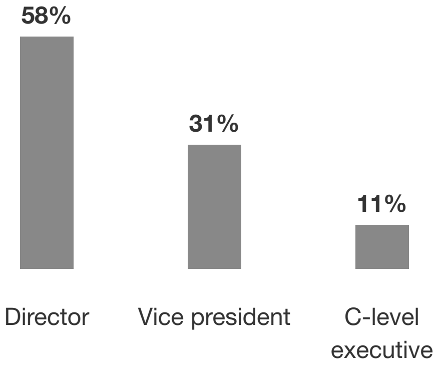
This spotlight is focused on the results of the 100 survey respondents and one interviewee from the manufacturing industry.

Appendix B: Demographics/Data

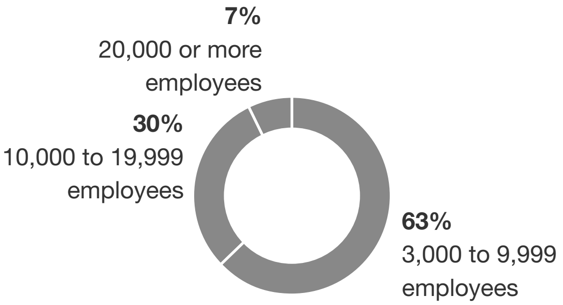
"In which country do you work?"



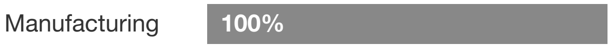
"Which title best describes your position at your organization?"



"Using your best estimate, how many employees work for your firm/organization worldwide?"



"Which of the following best describes the industry to which your company belongs?"



Base: 100 technology decision makers with responsibility over IoT security at US and Canada manufacturing firms
Source: A commissioned study conducted by Forrester Consulting on behalf of Armis, July 2019

Appendix C: Supplemental Material

RELATED FORRESTER RESEARCH

"The State Of IoT Security 2018," Forrester Research, Inc., January 9, 2018.

"The Top Security Technology Trends To Watch, 2019," Forrester Research, Inc., August 1, 2019.

"Best Practices: Securing IoT Deployments," Forrester Research, Inc., October 11, 2017.

"Protecting Industrial Control Systems And Critical Infrastructure From Attack," Forrester Research, Inc., April 19, 2018.

Appendix D: Endnotes

[1] https://www.securityweek.com/why-wannacry-was-wake-call-critical-infrastructure-security

[2] https://www.wsj.com/articles/one-year-after-notpetya-companies-still-wrestle-with-financial-impacts-1530095906

[3] https://threatpost.com/triton-ics-malware-second-victim/143658/

[4] https://doublepulsar.com/how-lockergoga-took-down-hydro-ransomware-used-in-targeted-attacks-aimed-at-big-business-c666551f5880

[5] Source: "Bridge The IT/OT Divide To Win With Smart Manufacturing," Forrester Research Inc., July 24, 2019

[6] From the United States' National Institute of Standards and Technology (NIST) and Center for Internet Security (CISO).

[7] Source: U.S. Attorney's Office, Middle District of Louisiana, "Former Systems Administrator Sentenced to Prison for Hacking into Industrial Facility Computer System," Department of Justice, February 16, 2017 (https://www.justice.gov/usao-mdla/pr/former-systems-administrator-sentenced-prison-hacking-industrial-facility-computer).

[8] Source: Kim Zetter, "A Cyberattack Has Caused Confirmed Physical Damage for the Second Time Ever," Wired, January 8, 2015 (https://www.wired.com/2015/01/german-steel-mill-hack-destruction/).

For more information, read the entire report: "State Of Enterprise IoT Security In North America: Unmanaged and Unsecured" at www.armis.com/forrester

Project Director:
Line Larrivaud,
Market Impact Consultant

Contributing Research:
Forrester's Security and Risk research group

ABOUT FORRESTER CONSULTING

Forrester Consulting provides independent and objective research-based consulting to help leaders succeed in their organizations. Ranging in scope from a short strategy session to custom projects, Forrester's Consulting services connect you directly with research analysts who apply expert insight to your specific business challenges. For more information, visit forrester.com/consulting.

© 2019, Forrester Research, Inc. All rights reserved. Unauthorized reproduction is strictly prohibited. Information is based on best available resources. Opinions reflect judgment at the time and are subject to change. Forrester®, Technographics®, Forrester Wave, RoleView, TechRadar, and Total Economic Impact are trademarks of Forrester Research, Inc. All other trademarks are the property of their respective companies. For additional information, go to forrester.com. [E-44072]