A Forrester Consulting
Thought Leadership Spotlight
Commissioned By Armis

September 2019

State Of Enterprise IoT Security: A Spotlight On Healthcare

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

FORRESTER®

75% of healthcare enterprise security professionals feel their current security controls and practices are not adequate for unmanaged and IoT devices.

"Just the possibility of someone being able to change the results a doctor might see, or to hack into medical equipment […], the effects would be potentially life threatening."

Medical device security project manager, US medical group

Introduction

From connected patient monitors to MRIs to life-saving medical equipment in hospitals, the internet of medical things (IoMT) is having a tremendous impact in the healthcare industry. While the billions of devices now deployed in healthcare have certainly helped to improve the quality and speed of patient care delivery, they have also increased the variety and severity of threats. In the past three years alone, it is estimated that IoT-related breaches in the healthcare industry have affected more than 135 million people in the US — or about 41% of the nation's population.[1] This is one reason the FDA issued guidelines in October of 2018 on strengthening the agency's medical device program to better protect patients.[2] Being fully aware of how much their industry relies on IoT, healthcare security professionals are on high alert: 85% are very-to-extremely concerned about these new risks. But are they doing enough to keep attacks at bay?

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, and three interviews with CISOs and IT project managers across various industries. This spotlight focuses on the results of the 98 survey respondents and the one interviewee from the healthcare industry.

KEY FINDINGS

› **Healthcare security professionals are extremely concerned about security exposures brought on by unmanaged and IoT devices, including connected medical devices.** Eighty-five percent are very-to-extremely concerned about the security risks posed by IoT devices, which was the highest proportion across all industries covered in our study. Specifically, one of their top concerns is the lack of authentication and authorization for access to unmanaged and IoT devices (66%). This fear is exacerbated by an increase in the use of unmanaged and IoT devices, further complicating their IT environment — for instance, improving regulatory compliance is the top factor driving the increase in IoT devices in the healthcare industry (65% versus 58% across industries).

› **They struggle to identify the risks and implement the right security solutions.** Fifty-six percent of respondents say they do not fully understand the risks associated with unmanaged and IoT devices. This is confirmed with an overall lack of awareness of respondents as to what qualifies as an IoT device — 48% think that MRIs, x-ray machines, and ultrasound machines which connect to the network are not considered IoT devices. This lack of clarity translates into challenges when it comes to buying and implementing solutions to effectively secure all connected and unmanaged devices — 49% of respondents struggle to navigate the changing/evolving nature of internal and external IT threats, 41% do not get the budget they need to invest in those solutions, and 33% report an unavailability of products/services that fit their needs (versus 26% across industries).

- **Investment in IoT security solutions is insufficient and needs to increase.** Seventy-one percent of healthcare security professionals feel that that their budgets for IoT security were inadequate relative to the risks they present. Their top IoT security priorities over the next 12 months include readying themselves for evolving threats (55%) and deploying an agentless security solution (47%).

DEFINING AN UNMANAGED OR IOT DEVICE

For this study, we refer to 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. They can include, but are not limited to:

	Healthcare-specific devices	Medical devices (patient monitoring systems, mobile imaging systems, infusion pumps, communication badges, etc.).
	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.
	Other industry devices	Industrial control systems (PLCs, HMIs, robotic arms, etc.).

The Fast Growth Of Unmanaged And IoT Devices Raises Concerns

With advances in medical care, healthcare delivery is getting more and more decentralized. Patients and providers are moving away from inpatient healthcare towards outpatient, and even virtual, interactions with their healthcare providers[3]. Healthcare executives are taking note, and also feel positively about the potential of connected medical and IoT to help them improve patient experience and increase revenue[4]. Also, more in-hospital medical devices are online and connected wirelessly, i.e., capturing and transmitting patient data and even delivering medical care.

In our survey of healthcare security professionals (see Appendix B), we found that:

- **Supply- and demand-side factors are converging to drive the growth of unmanaged and IoT devices in the healthcare industry.** With medical device manufacturers (i.e., suppliers) building more connectivity into different types of devices, and patients looking for more seamless experiences in their healthcare, healthcare delivery organizations are increasingly digitizing many of their operations. This includes introducing connected medical and IoT devices into their workstreams. These devices drive better tracking of patient medical status, information, and even the delivery of care. They are also heavily used in healthcare organizations to improve compliance with various regulations (e.g., reduce carbon emissions, improve worker safety, healthcare or financial transactions).
- **As a result, 81% have seen an increase in the use of unmanaged and IoT devices in the last 24 months.** The use of unmanaged and IoT devices is now so prevalent that 64% of surveyed respondents estimate that at least half of all devices on their enterprise network are unmanaged or IoT — including medical devices. To complicate matters, the speed of change has been fast as well: almost one in five (or 18%) estimate that the use of IoT devices has increased by more than 30% over the last 24 months. This trend is set to continue, with about half (47%) expecting that more IoT devices will continue to get introduced over the next 24 months.
- **Healthcare security professionals are aware of the increased risks that connected medical and IoT devices bring, and they are highly concerned with the growing security exposures.** Eighty-five percent of respondents report feeling very-to-extremely concerned about the security risks posed by unmanaged and IoT devices, the highest amongst all industries covered in the core study. In particular, they are most concerned about the leakage of patient data, viruses, as well as getting locked out of connected devices (as cited by the lack of authentication and authorization for access). However, their spending on security solutions has remained flat over the past 24 months, with the majority (66%) reporting a less than 5% increase in their IoT security spending.

While medical IoT is revolutionizing healthcare delivery and patient experience, the increased number of unmanaged devices offer little in the form of security, creating new security exposures for organizations.

78% of respondents has seen an increase in the use of unmanaged and IoT devices over the last 24 months.

"I think the number of devices touching the network that are not secure will continue to increase. As a consequence, we also believe the risk factor for those devices will increase,and the number of devices being hacked or manipulated will increase as well."

Medical device security project manager, US medical group

Lack Of Know-How, Skills, And Budget: The Basis Of Security Challenges

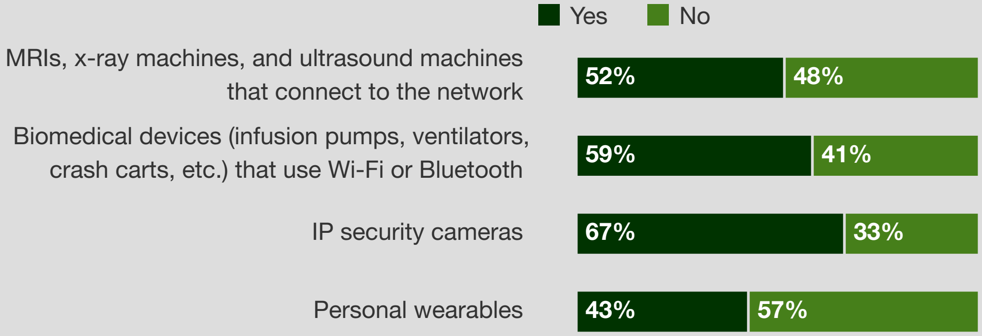
More so than in other use cases, the potential risks of failure and/or compromise are much higher when it comes to the use of unmanaged and IoT devices in healthcare. High-profile cases like WannaCry in 2017 and NotPetya in 2016 exemplify the far-reaching consequences of just a single orchestrated attack. Both of these attacks targeted hundreds of thousands of enterprise and healthcare systems, shutting down hospitals and medical equipment, and costing organizations billions of dollars to remediate, while putting public safety and human lives at risk. Despite the high publicity of such attacks, many healthcare organizations are still not doing enough to fully secure their IoT devices:

› **A growing majority see medical devices as unmanaged and IoT.** Fifty-two percent of surveyed healthcare security professionals believe that medical imaging machines that connect to the organization network are IoT devices (see Figure 1). They recognize the greater risk of breach, if they are not properly classified and protected. A significant proportion, 48%, still do not recognize these medical devices as IoT devices.

› **Still, healthcare security professionals are not fully aware of the risks inherent in unmanaged and IoT devices.** Only 43% agree that they "fully understand the risks associated with unmanaged and IoT devices," and only 56% have full visibility of the unmanaged and IoT devices that are connected to their network. Overall, the sentiment, as three-quarters of respondents agree, is that healthcare security professionals just "aren't sure where to start."

Figure 1

"Which of the following types of devices do you think can fall under the category 'Enterprise IoT'?"



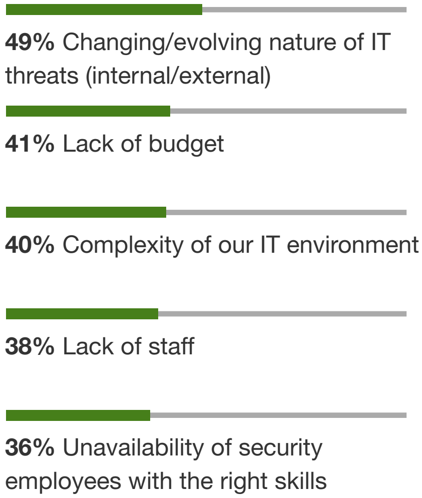
Base: 98 technology decision makers with responsibility over IoT security at US and Canada healthcare firms
Source: A commissioned study conducted by Forrester Consulting on behalf of Armis, July 2019

- **Lack of skills, tools, and budget all contribute to the inadequate approach to IoT security.** Despite growing awareness of the heightened risks, organizations are still not dedicating enough resources toward IoT security. Only half agree that they have the right skills and tools to effectively protect their unmanaged and IoT devices, and 81% feel that their spending on IoT security is not adequate. Lack of budget also surfaced as a top challenge when buying and implementing IoT security solutions (see Figure 2).

Overall, current practices are not enough to protect unmanaged and IoT devices, and 63% of respondents report having experienced related security incidents in the past.

Figure 2

“What are your top challenges when it comes to buying and implementing security solutions for unmanaged and IoT devices?”
(Showing top 5 responses only.)



Base: 98 technology decision makers with responsibility over IoT security at US and Canada healthcare firms
Source: A commissioned study conducted by Forrester Consulting on behalf of Armis, July 2019

Healthcare Organizations Must Increase Their Security Investments for Unmanaged and IoT Devices

Healthcare organizations must be prepared to address the security exposures stemming from the use of vulnerable unmanaged and IoT devices. This will address not only the new devices coming online to deliver medical care and run operations, but also the older medical devices running outdated operating systems that may not be properly updated, or even updatable. As suggested by security frameworks from organizations such as the United States’ National Institute of Standards and Technology (NIST) and the Center for Internet Security (CIS), a broad spectrum of security functions are required to properly secure unmanaged and IoT devices.

- **Healthcare organizations must allocate more resources to IoT security.** As organizations come to realize the extent of IoT security risks, they will need to rationalize the need to allocate more resources toward securing their unmanaged and IoT devices. Compared to other respondents, healthcare security professionals were more likely to admit that the level of spending on security for unmanaged and IoT devices is “somewhat or very inadequate” (71%). Ninety-five percent of healthcare security professionals project that they will increase their IoT security spending over the next 24 months, with the majority (39%) projecting a 11% to 15% increase.

- **Security professionals are prioritizing initiatives in line with their top concerns and challenges.** Their top IoT security priorities over the next 12 months include readying themselves for evolving threats (55%), gaining better control of connections to their networks (49%) and deploying an agentless security solution (47%).

95% of respondents plan to increase their budget dedicated to unmanaged and IoT devices security in the next 24 months.

Key Recommendations

As the use of unmanaged and IoT devices in healthcare continues to grow, so does the importance of implementing security solutions, practices, and controls that can identify and protect these devices. While there is no question of the value of connected devices in improving patient data integration and quality of care, improper and inadequate security controls of these devices put organizations and patients at risk of equipment downtime, data loss, costly remediations, etc. Furthermore, unlike in other industries, security breaches in the healthcare industry have the potential to disrupt medical care delivery and the effective treatment of patients. These potentially life-threatening breaches 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 healthcare security professionals about IoT security yielded several recommendations:

Assess and inventory your enterprise 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 emergency room to the operating room, to the nursing station to the accounting office. Use that information to build policies and implement tools to ensure devices are appropriately secured.

Prioritize device classification to identify 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 organization.

Raise awareness on growing IoT security risks. As an enterprise security professional, you need to demonstrate to decision makers in your healthcare organizations that unmanaged medical and IoT 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 solutions that provide device visibility, risk assessment, threat detection, and IoT-specific protection. Security professionals should create a comprehensive IoT security architecture that takes into account their organization's specific IoT use cases and security requirements. The challenge is that most traditional security products were built for traditional computers, and unfortunately they don't work for today's unmanaged medical 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.

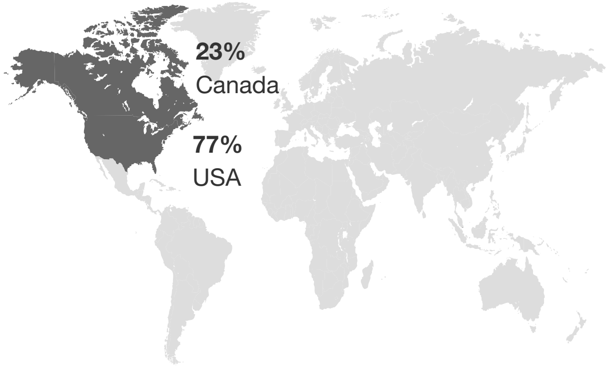
Appendix A: Methodology

This spotlight is based on a wider Thought Leadership study that looks 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.

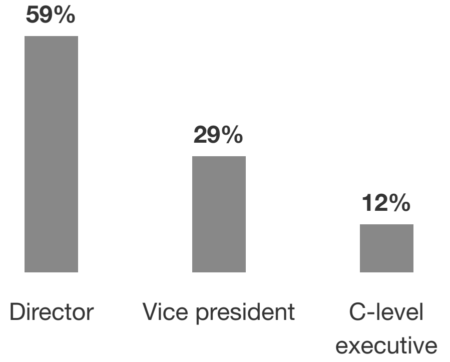
This spotlight is focused on the results of the 98 survey respondents and one interviewee from the healthcare industry.

Appendix B: Demographics

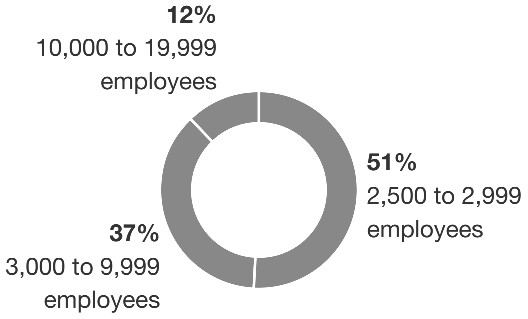
"In which country do you work?"



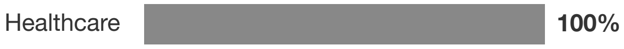
"Which title best describes your position at your organization?"



"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: 98 technology decision makers with responsibility over IoT security at US and Canada healthcare 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.

"Best Practices: Medical Device Security," Forrester Research, Inc., May 21, 2019.

"How To Build A Healthcare IoT Platform," Forrester Research, Inc., March 22, 2019.

Appendix D: Endnotes

[1] Source: "Best Practices: Medical Device Security," Forrester Research, Inc., May 21, 2019.

[2] Source: Scott Gottlieb M.D., "Statement from FDA Commissioner Scott Gottlieb, M.D. on FDA's efforts to strengthen the agency's medical device cybersecurity program as part of its mission to protect patients," U.S. Food & Drug Administration, October 1, 2018 (https://www.fda.gov/news-events/press-announcements/statement-fda-commissioner-scott-gottlieb-md-fdas-efforts-strengthen-agencys-medical-device).

[3] Source: May 30, 2019, "Build Your Healthcare IoT Platform" Webinar (https://www.forrester.com/webinar/Build+Your+Healthcare+IoT+Platform/-/E-WEB28365).

[4] Source: Forrester Analytics Global Business Technographics® Networks And Telecommunications Survey, 2018.

For more information, read the full study "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.