Securing the Single Biggest Threat to Healthcare IT:

IoHT and Connected Medical Devices
The Internet of Healthcare Things (IoHT) and connected medical devices are at the crest of a digital transformation wave rolling through the healthcare industry. IoHT technology encompasses a wide range of medical appliances, from consumer wearables to advanced AI platforms that analyze health data. By pairing data collection with diagnostic technologies, it offers an opportunity for healthcare providers to deliver patient-centric, customized care.

IoT (Internet of Things) adoption across all industries is steadily increasing, with the healthcare industry itself seeing a drastic jump—from 60% adoption in 2017 to more than 80% in 2019. This technology, however, is not without challenge. Security—often seen as IoT’s Achilles heel—threatens to obstruct wide-spread adoption as many healthcare providers struggle to reconcile the promise of improved patient care with ensured data security.
IoHT is on the Rise

IoT itself is on the rise across industries. 94% of businesses globally will be reliant on IoT in some form by the end of 2021—a 9% increase from 2019.

The healthcare industry, with its 20% jump in adoption in only two years, is no exception. Healthcare, an industry notoriously resistant to the adoption of newer technologies, is only slightly behind other automation-heavy industries such as manufacturing or retail when it comes to IoT adoption. This shows that healthcare leaders understand the potential of IoHT as an avenue for improved patient care through technology.
Security Concerns are Slowing IoT Adoption

Security is a universal concern surrounding not only IoHT adoption, but IoT in general. In 2019, 97% of companies across all industries mentioned security as a factor. Concerns center around three broad themes:

- Security software management (e.g., user authentication, password/credential management)
- Management of individual IoT devices and related software (e.g., tracking and managing IoT devices, security endpoints)
- Day-to-day training and maintenance (e.g., comprehensive training for employees, hardware/software tests and device evaluation)

![Chart showing types of IoT security considerations across all industries.](source: Microsoft)
For the healthcare industry in particular, security issues (e.g., privacy, cloud storage) remain key IoT barriers, only behind unavoidable challenges such as regulatory and budget concerns.

The healthcare industry’s increased caution regarding security is without a doubt warranted. Relative to other industries, healthcare has a stronger vested interest in IoT security issues. The healthcare industry is also one of the most frequently targeted by cyber attackers. More than a third (36%) of healthcare institutions have suffered downtime of at least five hours as a result of cyberattacks.

Sources: Healthcare IT News, Microsoft
Additionally, medical records are a rich source of identity theft, increasing their value on the black market. By some accounts, a medical record is up to 50 times more valuable than a credit card number. The average cost of a stolen record to a healthcare organization in 2018 was more than double the cost compared to the second most vulnerable industry, financial firms. And to top it off, most organizations with an active threat to their system often remain unaware of the issue for 18 months or longer.

**Average Cost per Compromised Record by Industry Sector**

- **Healthcare**: $429
- **Finance**: $210
- **Technology**: $183
- **Pharmaceutical**: $178
- **Services**: $178
- **Energy**: $165
- **Industrial**: $160
- **Education**: $138
- **Entertainment**: $132
- **Communication**: $132
- **Consumer**: $131
- **Transportation**: $130
- **Hospitality**: $123
- **Media**: $123
- **Retail**: $119
- **Research**: $117
- **Public**: $78

Sources: Ponemon Institute, D Magazine, Healthcare IT News
Investment and Expenditures in IoHT Security

The healthcare industry's expenditure on overall IT is in line with cross-industry averages. Healthcare spend on IT security, however, lags the industry average. As a share of the total IT budget, healthcare organizations on average spend 5% on security, below the cross-industry average of 6%, and well below rates in comparably sensitive sectors such as financial services (with a 7.3% spend) or software and Internet services (with an 8.7% spend).

Given the security challenges presented by increasing adoption of IoHT, as well as the cost of healthcare data breaches, cybersecurity spending in healthcare is expected to increase. A recent survey of healthcare executives finds data security ranked as the number one concern both in the immediate term and the near future.

Organizations are aligning their expenditures accordingly, with another survey of healthcare leaders finding that approximately 90% are increasing their cybersecurity spending each year, many by more than 5% each year.
IoHT Spending and Revenue

As healthcare leaders realize the value of investing more heavily in IoHT, expect to see explosive increases in IoHT investment. In 2021 healthcare providers will reach a 17% growth in IoHT spend over the previous five years. The healthcare industry as a whole is expected to spend nearly $54 billion on IoHT annually by 2029 (up from $21 billion in 2019).

While IoHT investment fosters better patient care, and drives security, it also creates new revenue opportunities for healthcare providers. It’s projected that the economic impact of IoHT devices could be between $170 billion to $1.6 trillion globally by 2025. The largest source of value is in the use of IoHT devices to monitor and treat illness, bringing in $170 billion to $1.1 trillion per year.
Device-Level Security

Device-level security is a particularly critical concern in the medical context, where device vulnerabilities can directly affect clinical care and patient safety. Within the IoHT stack, devices pose a significant security challenge, given the proliferation of device types and the different security configurations they offer. More than half of healthcare provider organizations have more than 50 different device vendors on their networks; over one-third have more than 100. As such, some analysts describe devices as “the single biggest threat to healthcare IT.”
By type of device, the most commonly used in healthcare settings are those with a 1:1 patient-to-device ratio, such as patient tracking or monitoring. Shared devices that are used for multiple patients, such as diagnostic or imaging systems, make up a smaller share of the overall number.

**MOST COMMONLY CONNECTED MEDICAL DEVICES**

- Patient ID & Tracking System: 38%
- Infusion Pump: 32%
- Patient Monitor: 12%
- Workstation: 6%
- Point-of-Care Testing: 5%
- Imaging System: 4%
- Medication Dispensing System: 3%

Source: Forescout
Based on the financial impact of attacks, device security should be a significant concern for the healthcare industry. In a 2019 survey, healthcare organizations reported that the impact of device-related attacks was nearly $350,000 on average per organization—higher than the cross-industry average and trailing only the transportation industry in size.
Organizations admit that the strongest motivation for increasing medical device security budgets would be external forces, such as a serious hacking incident at their organization or new regulations.

What would influence your organization to increase its budget for medical device security?*

- Serious hacking incident of your medical devices: 59%
- New regulations: 54%
- Concern over relationship with clinicians and other third parties: 25%
- Concern over loss of revenues due to security incident: 21%
- Concern over loss of patients due to security incident: 19%
- None of the above: 11%
- Median coverage of serious hacking incident of another company: 9%

Source: Ponemon Institute; * multiple responses allowed
Possibly, healthcare organizations are looking to device manufacturers to ensure protection against attacks. This assumption, however, would be mistaken. Device manufacturers are only slightly more likely than healthcare providers to have taken “significant” or even “some” steps to prevent attacks on the medical devices they produce.

**MEDICAL DEVICE SECURITY EFFORTS, BY ORGANIZATION**
More than one-third of both healthcare providers and device manufacturers feel that device security could be improved “greatly” and almost the entire remainder feel there is at least “some” room for improvement.

To what extent could the cybersecurity of the IoT devices your organization uses/manufactures be improved?

**DEVICE SECURITY – MANUFACTURERS VS. USERS**
Taking the Next Steps Towards Secured IoHT

Taking control of IoHT security must be top of mind for healthcare leadership, IT leaders.

**Take a Proactive Approach**
With 29% of healthcare organizations unable to instantly discover an attack, HCOs have no choice but to respond to attacks as they occur. Proactively solving for weaknesses now means patient data is more secure in the long run.

**Educate Employees**
In 2017, 80% of health IT executives and professionals reported that the greatest barrier to healthcare data security was poor employee awareness of security best practices. The healthcare industry is taking measures to address this, primarily through semi-regular security risk assessments, 74% of which involve some sort of security awareness training. However, a majority of such assessments only occur once a year or less. This level of training is likely not sufficient as individuals will not necessarily retain this information throughout the year.

**Implement Security Controls and Processes**
Many healthcare legacy systems lack essential cybersecurity controls. A comprehensive set of policies, procedures, and controls is essential for a secure network—especially if that network includes vulnerable endpoints like medical devices.

**Reduce Downtime**
Long downtimes for patching systems is a challenge because healthcare operations run 24/7. Other industries may be able to shut down their services for a few hours in the middle of the night to address security updates, but for the medical industry this puts patient lives at risk.

**Secure the Network by Containing Lateral Movement**
By understanding the root of security vulnerabilities and solving towards security, HCOs can remove barriers to continued progress and deliver increasingly valuable care to patients.

Health system networks often lack the basic segmentation necessary to limit lateral movement. If all devices can talk to one another and be accessed from the same points, accessing medical devices (and their data) through the network becomes dangerously easy.

Sources: Exscribe, Health IT Security, HIMSS
A Deep Dive into Network Segmentation and CMDB

Two areas imperative to every IoHT security strategy are network segmentation and configuration management database (CMDB).

Most healthcare organizations have attempted to roll out a network segmentation strategy, sometimes called zero trust segmentation, throughout their enterprise campus network. It requires in-depth knowledge of what is connected to the network in order to determine the proper policies for each device. Proper segmentation provides improved visibility and monitoring and is often the primary driver of medical device security. For example, without proper segmentation, a user of a hospital’s guest Wi-Fi could gain unchallenged access to critical systems and patient data. Because digital transformations often require enterprises to pivot on technology strategy, there are many challenges to overcome. The most common challenge is the presence of legacy systems, with more than a third of enterprises experiencing this hurdle. Nearly a quarter cite this as their most difficult challenge.
Segmentation isolates and filters network traffic to limit and prevent access between network areas, VLANs, or even individual switchports. There are several ways to approach network segmentation, all dependent on how granular the isolation needs are. Segmentation, in a traditional sense, can be managed with firewalls and access-lists segmenting specific VLANs and subnets. But to truly prevent lateral movement, switchports can be isolated with Network Access Control (NAC) solutions such as Cisco ISE (Identity Services Engine). NAC allows for dynamic profiling of every switchport and dynamic application of access-lists per device type. Ultimately, a roll-out of a NAC solution comes with many challenges. Where many roll-outs fail is with a less-than-full understanding the different medical devices that need unique profiles. This is where a mature CMDB comes into play. Having a robust CMDB helps the network segmentation strategy become successful. Without visibility into what is attaching, it is hard to determine where access should be allowed. Network segmentation tools usually don’t have a robust database containing the many medical devices that will attach to the network, therefore leading to many “unknown device” scenarios and gaping holes in the security policy. The CMDB will help achieve a more precise inventory of what is actually on the network.
By collecting and documenting a centralized source of truth, it allows organizations to fully understand their medical device inventory. Contributing to a CMDB allows organizations to understand who owns and supports each device, but most importantly it provides access to data that helps identify risks.

Leveraging ServiceNow Discovery and CMDB, and committing to maturing the data allows for more fruitful and reliable data within the ServiceNow platform (i.e. ITSM, GRC, etc.). In the example of ServiceNow, there are also plugins to help enrich the medical device data even more, which then allows for firmware management and patch management. This is really the first line of defense in medical device security—a proper understanding of what you are securing in the first place.
AHEAD Builds Platforms for Digital Health

From serving more informed and empowered patients, to fending off industry disruptors, to providing quality remote care during a global pandemic—it’s never been a more urgent time for healthcare providers to transform. And the industry is responding.

AHEAD currently helps more than 60 health systems with their digital transformations. Healthcare transformation involves much more than project by project updates to technology. It involves fundamental changes in culture, communications, operations, and not least of all, the underlying infrastructure. Without the right foundation in place, your digital health initiatives can impact lives.

We created our digital delivery platform to enable change and innovation for the healthcare industry.

To learn more about AHEAD’s Healthcare Practice, visit ahead.com/digital-healthcare/

National Hubs

www.ahead.com

ATLANTA
1117 Perimeter Center
W406
Atlanta, GA 30338

CHICAGO
401 Michigan Ave.
#3400
Chicago, IL 60611

NASHVILLE
5300 Virginia Way
Brentwood, TN 37027