



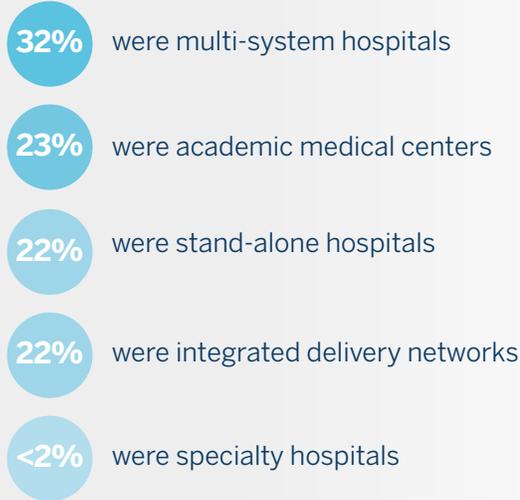
## Operational Technology Security and the Internet of Medical Things: Protecting your patients, privacy, and equipment

The importance of Information Technology (IT) security to healthcare organizations cannot be overstated. Guarding their network against ransomware-related issues and other attacks is a high priority. In comparison, the attention to and investment in Operational Technology (OT) security pales even though healthcare executives and IT personnel recognize the vulnerabilities posed by their connected medical devices, facilities, and other equipment.

The disconnect between awareness of the dangers of unsecured device networks and the actions taken to protect them is evident in research conducted by The Healthcare Information and Management Systems Society (HIMSS) in March and April 2021. **In a survey of 60 hospital systems, medical centers, and delivery networks, most reported having concerns about their OT security – but noted that their organizations invest very little to remediate the threat.**

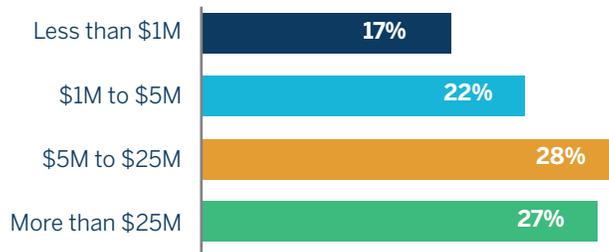


OF THE ORGANIZATIONS PARTICIPATING IN THE SURVEY:



Nearly half (42%) of the 60 survey participants have an annual overall IT budget of less than \$5 million, while one in five (20%) has an annual IT budget of more than \$5 million. The average overall annual budget for IT is almost \$13 million (IoT/IoMT Security, Healthcare Information and Management Systems Society, April 2021).

ESTIMATE OF OVERALL IT BUDGET:   
Average IT Budget  
**\$12,727,000**



The security of IT devices such as laptops, servers, and other equipment that connect to healthcare systems' networks is a priority for providers. It safeguards their data, patient privacy, and proprietary information. The value of protecting this information is well understood, and the financial commitment of these organizations reflects that priority.

But what about security threats adjacent to IT that can prove to be just as damaging but often receive little to no investment or intervention?

## Meet the IoMT (Internet of Medical Things)

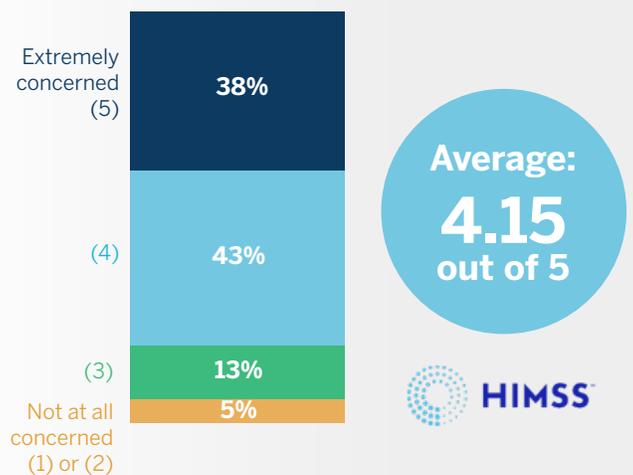
The Internet of Things (IoT) and Internet of Medical Things (IoMT) encompasses a healthcare system's non-IT assets, such as medical, lab, and facility equipment. Each device has access not only to patient data but to patients themselves. For example, when an MRI machine malfunctions or is exploited by an outside party to obtain sensitive data or penetrate the network, security teams may be alerted – but not before the patient in the process of receiving the MRI is affected. And, medical information – which may be critically needed to offer results or a diagnosis – may be delayed or lost.

Devices and equipment that fall under the umbrella of operational technology (OT) are managed by a specialized group of clinical engineers. But medical devices have historically had no security mandate. Device security is often up to the discretion of the healthcare organization's infrastructure. This potential gap in security means that medical devices create vulnerabilities for healthcare systems – threatening data, security, and patient safety.

## The Great Divide: Between Awareness and Action

Survey participants openly acknowledge the threat posed by unsecured medical devices.

LEVEL OF CONCERN ABOUT THREATS TO OPERATIONAL TECHNOLOGY

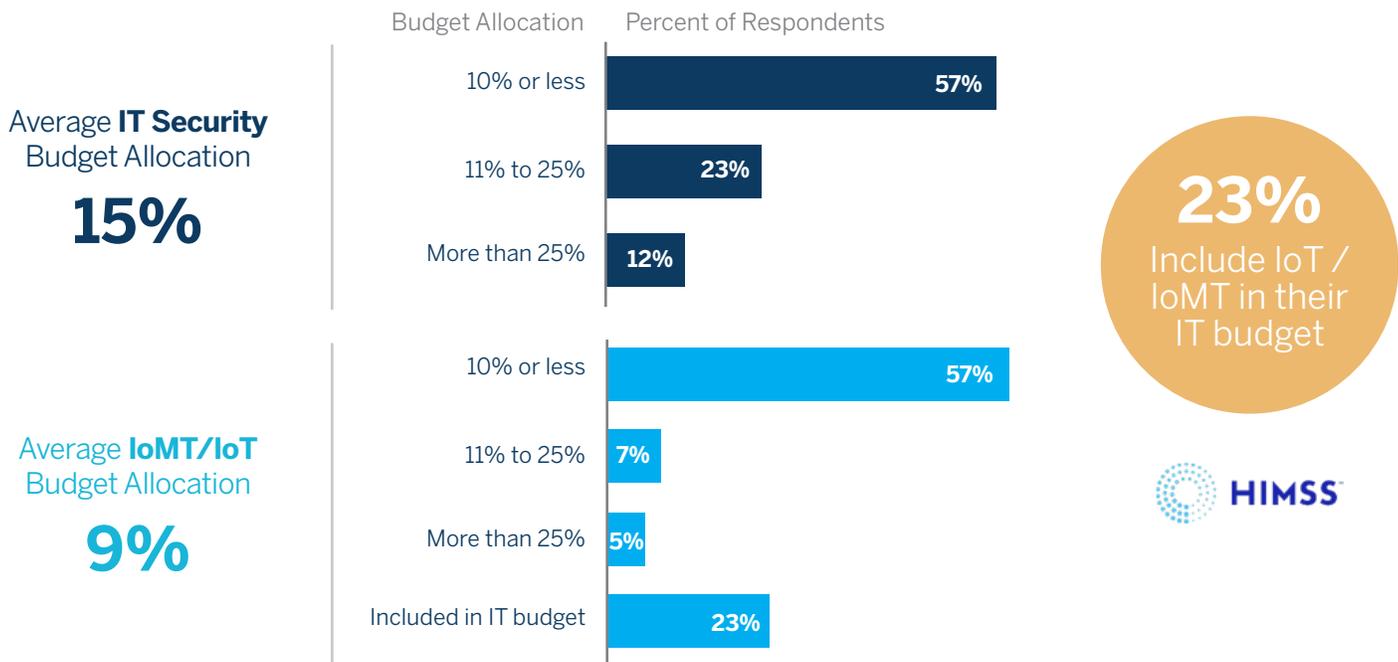


OF THOSE SURVEYED BY HIMSS IN MARCH 2021:

- 80%** 80% report concerns regarding security attacks to medical devices.
- 51%** 51% of IT managers and IT security personnel are extremely concerned.
- 20%** 20% of executive leaders are extremely concerned.



However, a disconnect emerges when comparing the investment healthcare systems make to secure their medical device networks,



IT security, on average, receives a 15% allocation of a healthcare system’s overall IT budget. IoMT/IoT security receives less – 9%. **In fact, 3 out of 4 (77%) of healthcare systems surveyed don’t include OT security in their IT budgets at all.**

**Why, when awareness is high, does action lag so far behind?**

Closing the OT security gap requires a financial and organizational

commitment. Both can be barriers – not necessarily because of a lack of funding available for security, but due to a lack of knowledge about how to deploy it. For instance, a healthcare system may not have an OT security team if management expects that these roles fall under the governance of IT. Or a clinical engineering team may not have representation at the C-Suite level, and therefore may not have the opportunity to influence the allocation of resources and spending for OT security.

Securing OT may require collaboration between clinical engineering and IT teams, along with new processes and new technologies. Bridging this gap can prove challenging, particularly among larger healthcare systems with multiple sites, inter-state locations, and remote or field teams.

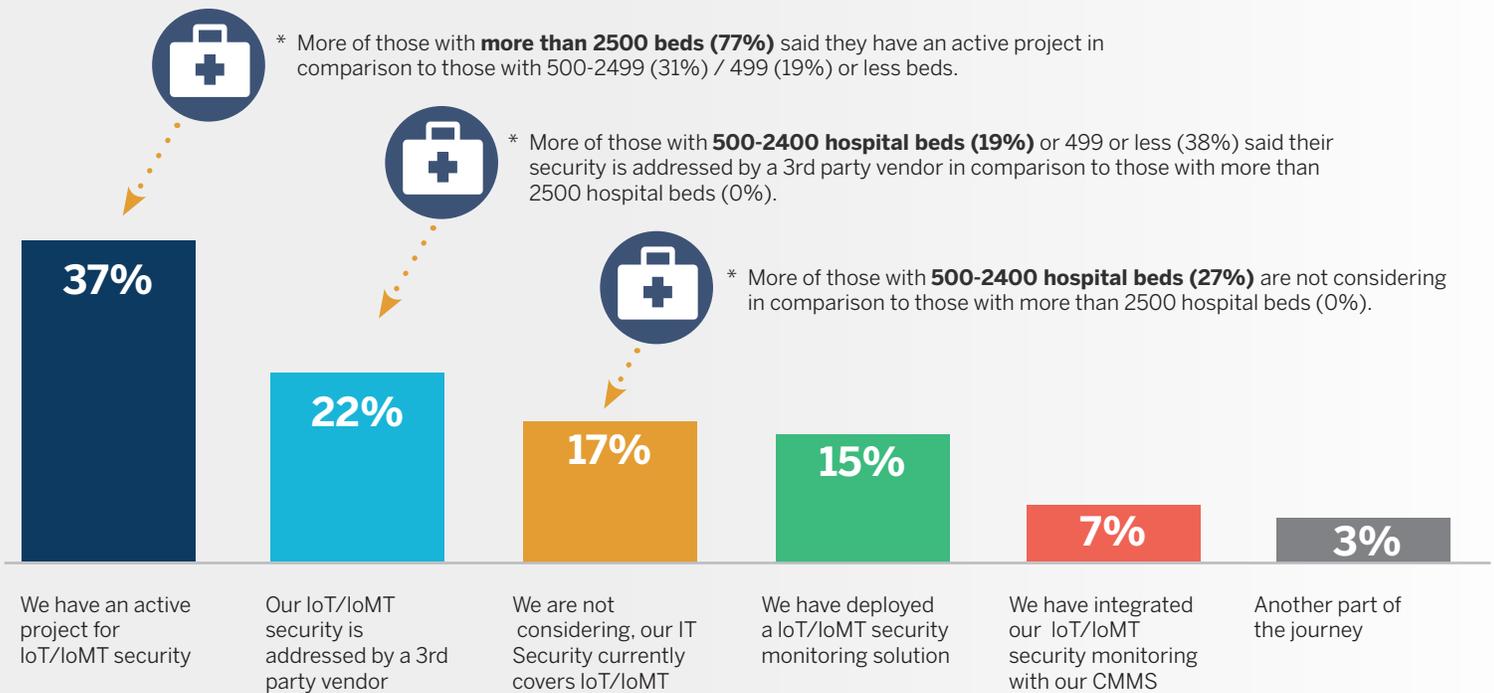
**And, healthcare organizations may not know where these gaps in their systems lie.**

# The IoT/IoMT Security Journey

Of those surveyed by HIMSS in March 2021, the larger the healthcare system, the more likely they are to be addressing the gap to secure their OT through an active project. This may be due to awareness of the issue or their ability to make the necessary financial and organizational commitments.

The survey revealed that larger percentages of medium to small hospital systems rely on third party vendors to manage their IoT/IoMT security. While more effective than doing nothing, many third-party OT security monitoring tools stop short of offering what healthcare systems require to make their OT security effective: response and remediation.

## HEALTH ORGANIZATIONS' PLACEMENT ON THEIR IOT/IOMT SECURITY JOURNEY



Base: Total Respondents: n=60

\*Please note these are significantly different in the data but should be interpreted as directional due to low N size.

# The Solution: Intelligence Hub and a System of Action

Creating a secure medical device network is a three-step process: discovery and monitoring, inventory, and orchestrated remediation.



## Step 1: Discovery and Monitoring

Monitoring the function of every device on a healthcare system's network is no easy task. That's why OT monitoring tools are vital to accomplishing this step.

Software solutions that search and discover a healthcare system's OT network are integral to maintaining medical equipment and devices, and to raising security issues to IT teams when they arise. But further action is needed to successfully remediate these issues, ensure device safety, and support optimal utilization of medical equipment. What's more, OT security monitoring tools can't discover devices that have yet to be onboarded or are in storage. These devices may still have vulnerabilities that need correcting before they join the connected medical fleet.



## Step 2: Inventory

A device inventory, or single source of truth for device technology, allows for the easy identification of every device in a healthcare system's IoMT. Without a streamlined device inventory, multiple systems, files, and spreadsheets may be used to keep track of devices.

Some tracking systems may contain incomplete or confounding information.

For example, an entry for a specific machine may include only the name of the manufacturer. When a security or operations issue with that piece of equipment arises, such incomplete information may make it difficult to identify the owner, location, or even type of the machine. Therefore, the threat level cannot be identified, and the right course of action cannot be determined. For instance, if a security threat is detected on a machine providing life-saving support, and the standard response is to disable the machine, the outcome could be fatal.

A complete inventory – a single platform that contains detailed device profiles using standard naming conventions and data fields – allows for the tracking, sharing, and management of devices. Accurate accounting of each device's usage and availability precludes inefficiencies, wasted resources, and a backlog in patient care. And it can be vital to protecting the health and safety of patients. In addition, this inventory contains all devices – connected or not.



## Step 3: Orchestrated Remediation

Once a security flag is raised, the appropriate course of action must be taken. A lack of communication between IT and technician teams may make it difficult to determine who is responsible for fixing the problem. And, a lack of insight into the nature of the issue – for example, an inability to locate the device or determine the threat level, may make it impossible to respond appropriately or in a timely fashion.

For hospital systems that operate across numerous sites or a large geographical area, dispatching the right field technician may be complicated enough. Additionally, some devices require maintenance to be completed by their own support teams.

Medical equipment is expensive. The loss to a healthcare system's bottom line – and the resulting damages to patient outcomes – due to devices being offline until the right person can be identified, located, and dispatched to fix them, is significant. It is also avoidable.



## Nuvolo OT Security for Healthcare

Nuvolo's out-of-the box integration with OT discovery and security monitoring tools provides a three-step, SaaS-based solution to operational technology issues.

Cloud-based software seamlessly integrates with third party discovery and security monitoring tools, picking up where they leave off to create a detailed inventory of a healthcare system's medical devices. Through shared naming conventions and standardized data formatting, Nuvolo is able to create a common data model from a healthcare system's device inventory. Then, to funnel this information into a single trusted data source: a centralized intelligence hub.

This intelligence hub logs the device information, owner, location, maintenance history, software information, and usage of every device. And, because it relies on a cloud-based platform, all of this identifying information is accessible from anywhere to clinical engineering, IT, security, as well as field and support teams.

When a security issue arises, Nuvolo is able to automatically initiate the appropriate remediation workflow by creating a work order to dispatch a qualified technician or security engineer to respond. Because each device is known and fully inventoried, the response can be prioritized based on the severity of the issue and the number of devices it is affecting. Therefore, patient health can be prioritized.

With Nuvolo's out-of-the box software solutions, healthcare systems of all sizes can ensure the safety of their medical devices, and make sure that each device is receiving optimal utilization. That means less time spent out-of-service waiting for repairs, as well as better monitoring of a machine's availability. The intelligence hub can tell a provider when a machine is being used and when it is available, so that it can be dispatched appropriately for patient care.

Nuvolo can also help organizations bridge the gap between operations and security teams. Through automatically generated work orders, responsible parties will be notified and called to action when a network device needs to be serviced or when a security threat is detected. All maintenance done on a machine will feed back into the inventory, so that every maintenance visit is tracked – both for records and compliance. Likewise, all software updates and informational technology activities will also be automatically tracked, simplifying processes for IT teams.

Nuvolo offers the promise of a fully connected workplace for healthcare: where Health Technology Management, IT, facilities, pharmacy, and clinical teams and more collaborate on a single, integrated platform to support patients, clinicians, and your entire organization.

Find out more at [Nuvolo.com/healthcare](https://www.nuvolo.com/healthcare)

