How Vulnerable is Your Hospital to Cyberthreats?

By Dr. May Wang, co-founder and CTO, Zingbox Inc.

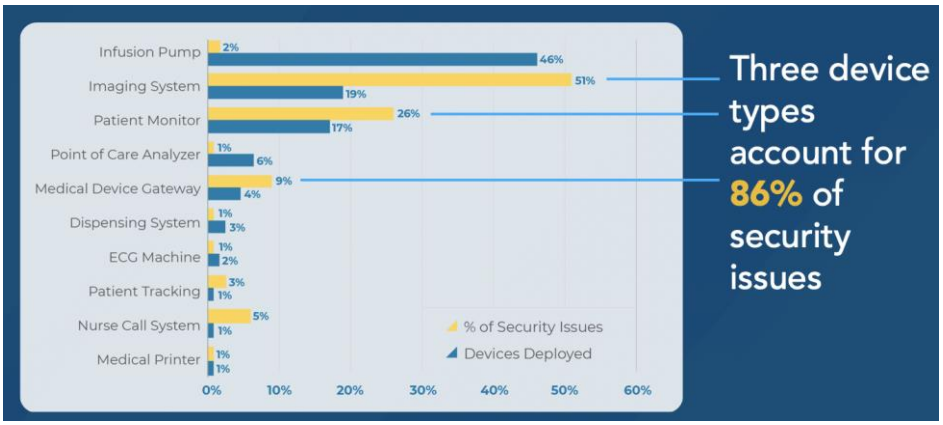
Do you know the top three medical devices that account for nearly 86% of all hospital security breaches? Or the common security issues that leave these devices vulnerable? Are you aware of how healthcare organizations use VLANs to secure medical devices and the industry best practices for deploying them?

These are some of the issues examined in a newly completed threat report conducted by Zingbox over a year-long research study. With the largest client base in healthcare and 1.6+ petabytes of analyzed IoT data per day, Zingbox is in a unique position to glean insights and best practices from hundreds of healthcare organizations and summarize the research results in the threat report.

Vulnerability of Connected Medical Devices

With the rising number of IoT devices connected to the network on a daily basis, many healthcare organizations want to know "what's on my network at this very moment?" The ability to inventory all connected devices—both medical and non-medical—in real-time is one of the biggest challenges they face and an important consideration when

choosing a solution. The threat research started by looking at the most commonly connected medical devices in over one hundred hospitals.



Devices with Most Security Issues

As shown in the above chart, while infusion pumps are the most widely deployed (46%) medical device, they account for only 2% of security issues. On the other hand, imaging systems comprise only 19% of medical devices deployed, yet account for more than half (51%) of all security issues. These findings help healthcare organizations understand the most vulnerable devices in their networks, enabling them to provide protection for potential cyberthreats appropriately.

Protection with VLANs

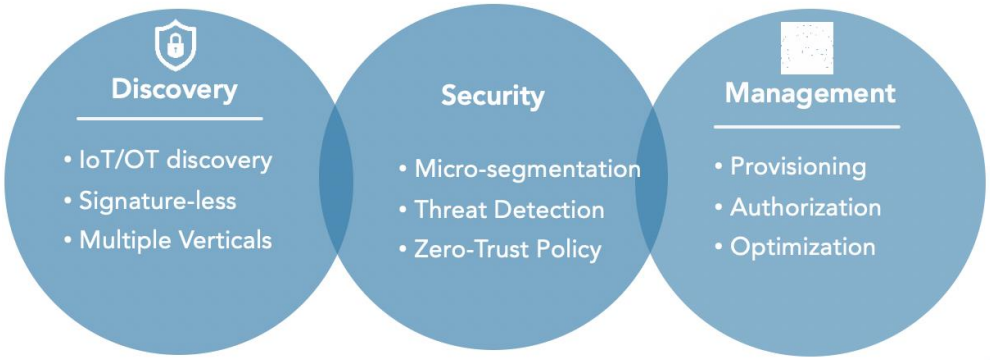
We also looked at how widespread the use of medical VLANs are and the best practices for implementing and maintaining them. The good news here is that hospitals employing 20-49 VLANs increased from 10% in 2017 to 36% in 2018. Unfortunately, the study also found that medical devices are oftentimes spread across multiple VLANs. For example, imaging systems account for 19% of all devices deployed, but are spread across 54% of VLANs making them harder to manage and protect. The ability to efficiently use VLANs to provide access control, and thereby protection from cyberthreats, has become a challenge that many healthcare organizations face.

Additionally, while many hospitals are increasing the deployment of VLANs, only 3% of VLANs are used exclusively for medical devices. The majority of VLANs (72%) include a mix of medical, non-medical (e.g., IP phones, cameras, printers) and IT devices.

These connected non-medical devices can pose serious security issues. For example, cameras account for less than 5% of devices, but represent 33% of all security issues. Being able to see those connected non-medical devices and their behaviors on the network continues to rank at the top of hospitals' security list.

Automated IoT Lifecycle Management

The results of this latest study further validate the Zingbox approach to secure and manage connected IT/IoT devices in the healthcare environment. Powered by AI and deep learning technologies, the recently announced Zingbox IoT Command Center is the first solution of its kind encompassing the discovery and security of IoT devices as well as the management and optimization of the entire IoT lifecycle. It helps healthcare organizations to not only discover, but secure and manage the device lifecycle with in-depth operational insights to increase patient safety, improve work efficiency, and reduce TCO.



Zingbox IoT Command Center

For additional insights, please watch the webinar hosted by The HIMSS Learning Center. Sign up here to download the Zingbox 2018 Threat Report and receive the new Zingbox 2019 Threat Report as soon as it is available.