BioMedical & Clinical Engineers

Cybersecurity Preparedness Factbook

FORESCOUT®

TABLE OF CONTENTS

THE GOAL OF THIS FACTBOOK IS TO PROVIDE A COMPREHENSIVE AND AUTHORITATIVE REVIEW OF CURRENT HEALTHCARE IT PRACTICES AND CYBER PREPAREDNESS.

BACKGROUND

The information and statistics referenced in this report are extracted from a variety of sources including multiple independent publications, consulting firms, and associations, as well as Forescout field statistics and anonymized metadata extracted from the Forescout solution.

Third-party statistics will also be accompanied by a citation of the source so that credit may be duly attributed and so that the reader is given a basis for further investigation.

Using this factbook, hospital administrators should be able to get a good sense of where they stand and how they stack up in the industry on matters of technology investment and cyber preparedness. More important still, we trust this will provide administrators with specific steps to take to shore up their security posture.

INTRODUCTION

An enterprise thousands of years in the making, healthcare is now in the throes of a frenzied modernization campaign. Spurred by legislation, business pressures, better data responsiveness, and the promise of expanded medical capabilities, today's hospitals are not just digitizing their business management and data management processes, they are networking everything. From managing a broad range of traditional medical instruments, to building digital interfaces with often unseen (and complex) software interactions, they find themselves tasked with connecting technology to every point of care.

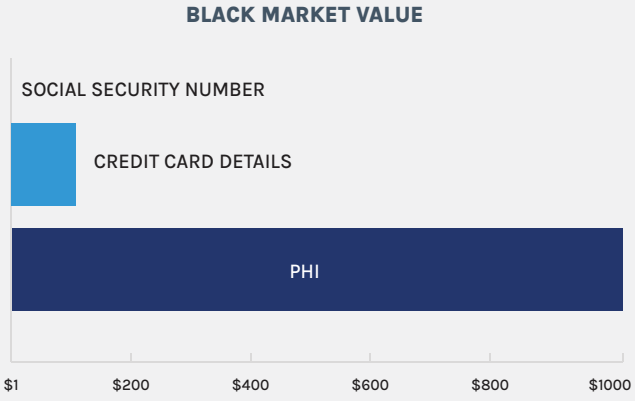
Because so much high technology has been so quickly outfitted on top of infrastructure, processes, and staff born of a different era, many hospitals are struggling to manage it all. The incredible size of many healthcare organizations, sprawling layouts, and continuous mergers and acquisitions only add to the challenge. It's likely that no single manager knows how all the pieces interconnect, let alone how they should connect.

The margins where different roles and responsibilities touch are likely to get confused. Stakeholders operating out of the same ecosystems may work according to standard operating procedures in their own disparate and closed loops. It can easily go unnoticed if a new device or different architectural wrinkle introduces additional vulnerabilities to the network. Incongruent or outdated policies and procedures might be difficult to pinpoint and persist even as they contribute to a slow and inefficient working environment. Administrators might not even know what assets the hospital has at its disposal or where they're located.

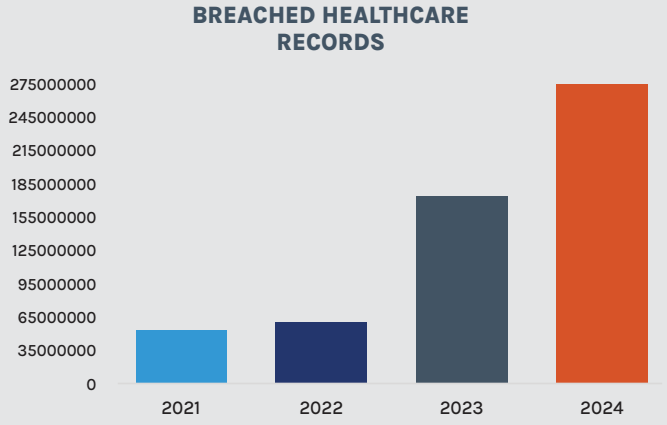
With this level of digital disarray inside hospitals, smart administrators might look to broader industry benchmarks and accepted best practices as they endeavor to get a handle on the situation and meet chaos with clear-minded control. Unfortunately, there are none, which is precisely why we've compiled this factbook. We hope this helps you navigate through standard practices, best practices, technology investment rates, and general security incidents.

Hospitals represent a rapidly changing frontier at the intersection of science and technology.

Hospitals have a target on their back.



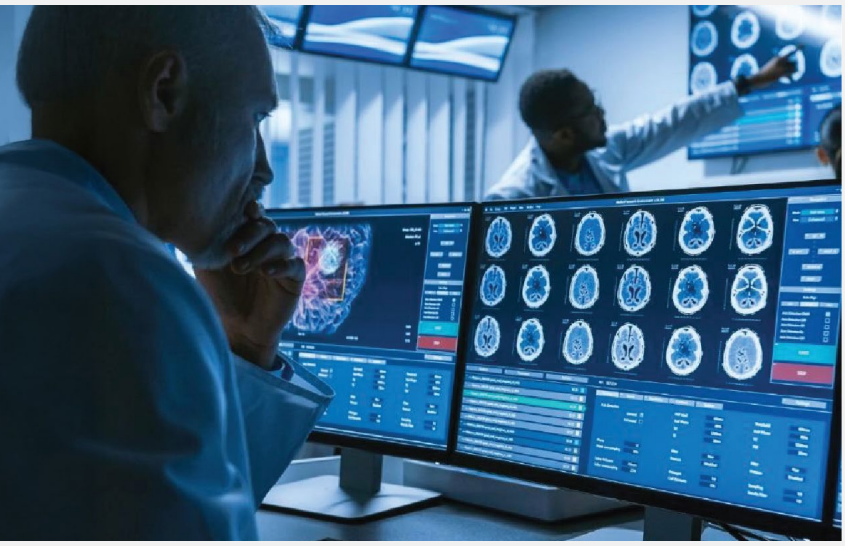
Medical information and health research data fetch a high price on the black market — as much as $1,000 per record. (Compared to $1 for a social security number and $110 for credit card details.) [1]



275M individual medical records were breached in 2024 – representing a more than 63% increase over the year prior. [2]

[1] CBS NEWS; Hackers are stealing millions of medical records — and selling them on the dark web

[2] U.S. Department of Health and Human Services, Office for Civil Rights



- Healthcare is one of the most cyber-targeted industries, with **23% of all US data breaches in 2024** occurring in the healthcare vertical. [3]
- **47%** of HDOs acknowledge that they don't have enough budget for a comprehensive cybersecurity program. [4]
- **9 of the 10** largest healthcare breaches in 2024 were attributed to a hacking or IT incident. [5]
- Only **49%** of hospitals in the U.S. state that they adequately manage or cover third-party supply chain risks. This is critical as **46% of these hospitals claim a ransomware attack was caused by a third-party.** [5]

Nearly 75% of hospitals reported have experienced a cyber incident in the last 12 months.[6]

- Ransomware attacks against the healthcare sector in the US increased **128%** in 2023. [7]
- **68%** of healthcare organizations say that ransomware attacks disrupted patient care. [4]
- Only **47%** of HDOs say their organization is prepared to prevent and/or respond to an attack on a medical device. [4]
- Ransomware attacks decrease hospital volume up to **26%** during the week of the initial attack. [8]
- Admitted patient mortality rate increases by up to **41%** when a ransomware attack begins. [8]

[3] Kroll; Data Breach Outlook 2025

[4] Ponemon Institute; Cyber Insecurity in Healthcare

[5] Department of Health and Human Services Office for Civil Rights data breach portal

[6] HIMSS; 2024 HIMSS Healthcare Cybersecurity Survey

[7] Office of the Director of National Intelligence; Ransomware Attacks Surge in 2023; Attacks on Healthcare Sector Nearly Double, Feb. 2024

[8] University of Minnesota School of Public Health; Hacked to Pieces? The Effects of Ransomware Attacks on Hospitals and Patients, Oct. 2024

THE ATTACK SURFACE IS HUGE, INCREASING THE RISK TO PATIENT SAFETY

The number of connected devices is growing at hyper speed, expanding the attack surface and making it difficult to scale security. These devices include healthcare devices like patient tracking and identification systems, infusion pumps and imaging systems. It also includes infrastructure devices such as building automation systems, physical security systems, uninterrupted power supplies, backup generators and other OT systems and devices that are increasingly joining IT networks.

UNDERSTANDING AND PRIORITIZING RISK

The convergence of the clinical, IT and OT networks creates a new class of security risks. Cybercriminals can now move laterally across any of them. The increase in mergers and acquisitions, which are prevalent in the healthcare sector, further amplifies these security challenges. Much like clinical diagnosis and treatment, CISOs must detect risks early and prioritize the best course of action. Security and risk management teams that attempt to mitigate every risk will realize marginal results. Additionally, biomedical teams are responsible for managing thousands of connected medical devices. By fully understanding threats on the network and pinpointing the devices that are harboring the most risk, it's possible to maximize productivity, increase ROI and reduce risk across the network.

- US hospitals average between 10-15 connected medical devices per bed.[9]
- There are 6,120 hospitals across the US.[10]
- There are 916,752 hospital beds throughout the US.[10]
- That equates to nearly 14 million connected medical devices in U.S. hospitals, an average of approximately 2,250 connected medical devices per hospital.

38%
of medical devices are exposed to some degree of cyber risk

26%
of infusion pumps have critical unpatched vulnerabilities

10%
of Windows-based medical devices have active anti-malware running

246%
more DICOM servers exposed to the internet since 2017

[9] HIPAA Journal; Mar. 2024

[10] American Hospital Association; Fast Facts on U.S. Hospitals, Jan. 2024

CLASSES OF DEVICES ON MEDICAL VLANS

Many networks still operate in organizational silos, leaving gaps in security. Clinical engineers often focus on securing connected medical devices while facilities and operations teams concentrate on securing building automation systems. Given these siloed priorities, who is responsible for looking at security holistically? At the most basic level, healthcare organizations need to be aware of the Clinical, IT, IoT and OT devices connecting to their networks. This awareness helps to break down security silos, brings the right groups together to discuss security strategies, and provides the foundation for a holistic approach to security. The classes of devices will likely shift in size as more medical devices connect to networks, making it critical to regularly review and adapt security strategies.

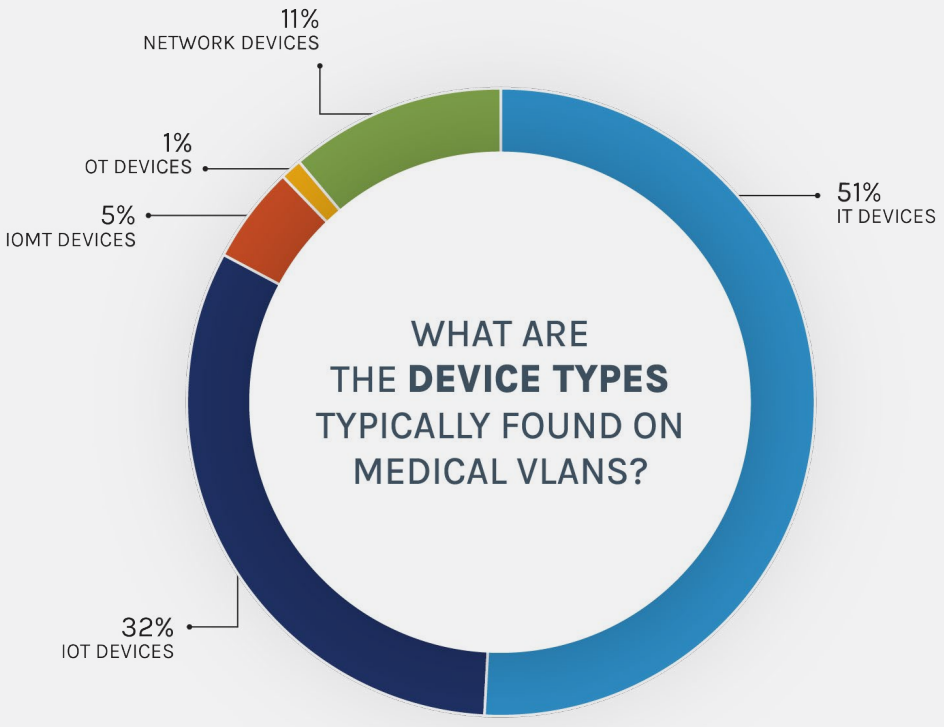
- IT devices: Personal computers, laptops, purpose-built workstations, servers, thick and thin clients, virtualization hypervisors and enterprise networking gear

- IoMT and OT devices: Medical devices, critical care systems, building automation/HVAC systems, power generators, badging and other facilities-related devices as well as IP-enabled security cameras and physical security systems

- IoT devices: VoIP phones, network printers, mobile devices, tablets, controllers and converters, video conferencing devices, presentation systems, smart TVs, entertainment consoles, various accessories

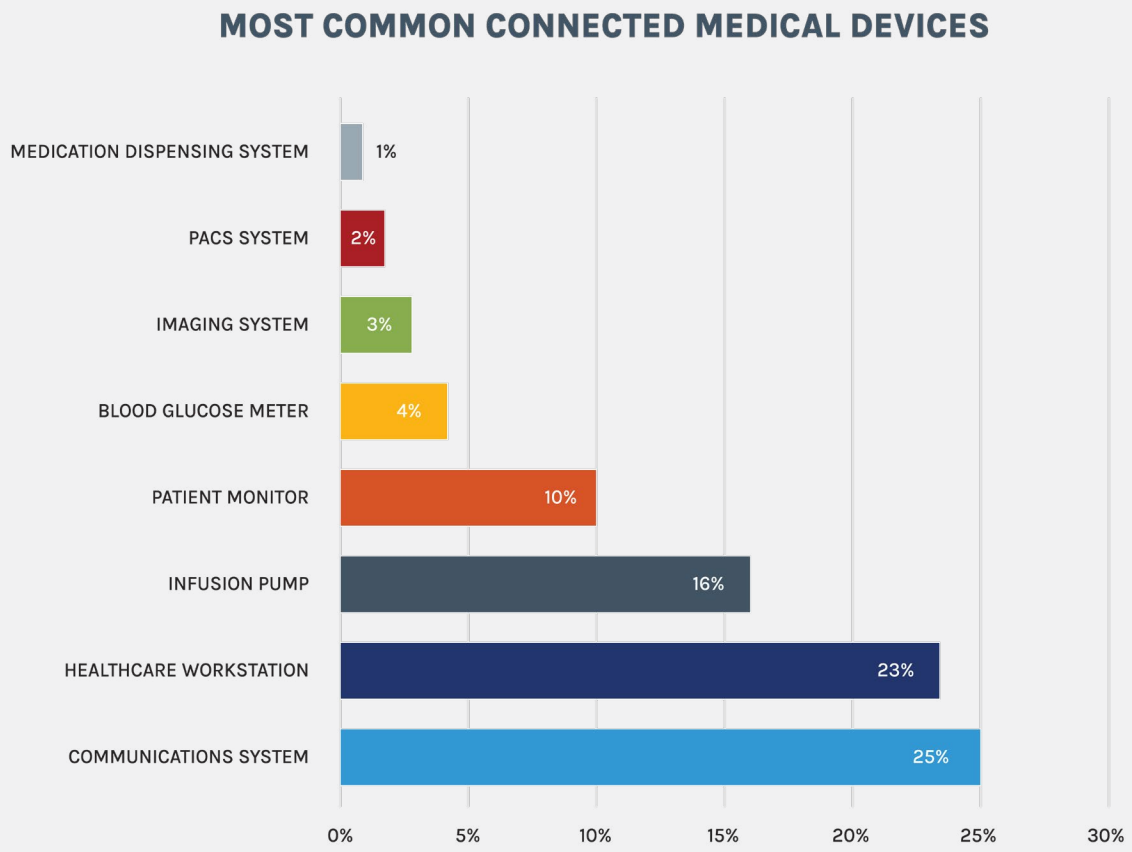
Hospitals try to contain and manage cyber risks primarily through the use of VLAN segmentation regimes.

The total number of VLANS configured within hospital networks typically range between ten to over a hundred.



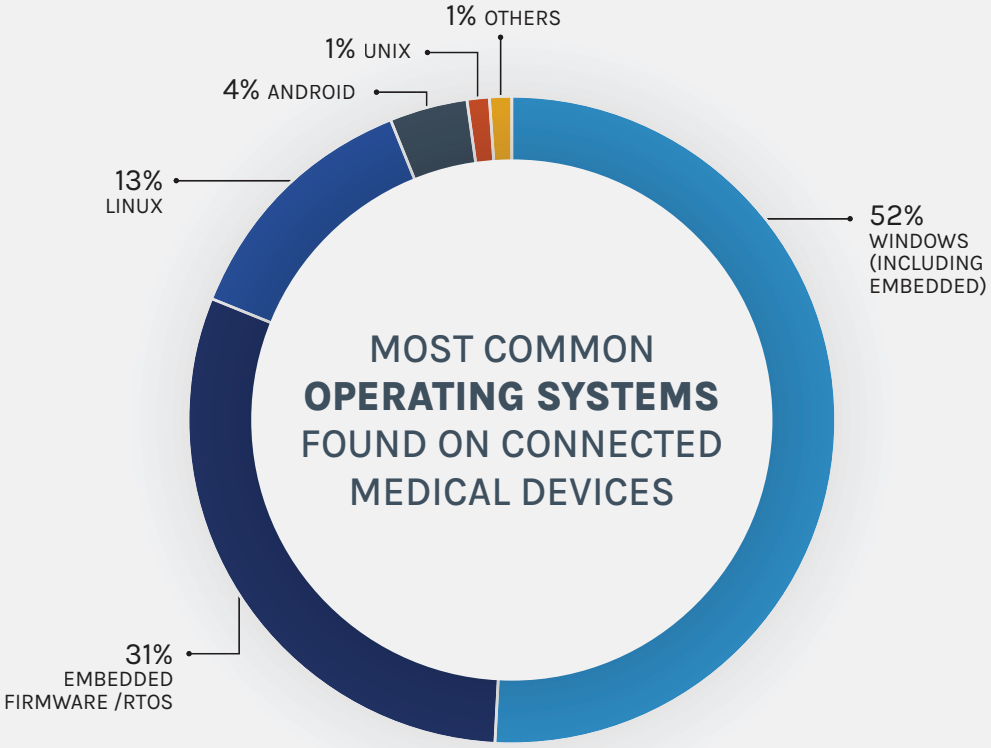
THE MOST COMMON CONNECTED MEDICAL DEVICES

Inpatient medical facilities tend to see a higher percentage of devices that are “connected” to a patient. Per-patient devices such as patient identification and tracking systems, infusion pumps, and patient monitors represent most of the healthcare devices on clinical networks. This makes sense as they are the devices tracking and monitoring patients on a 1:1 ratio. Devices such as those used in laboratory diagnostics or medical imaging represent a smaller number because they are shared devices. These more expensive systems tend to become long-lived legacy devices that are challenging to patch and keep updated.



DIVERSITY OF DEVICE OPERATING SYSTEMS

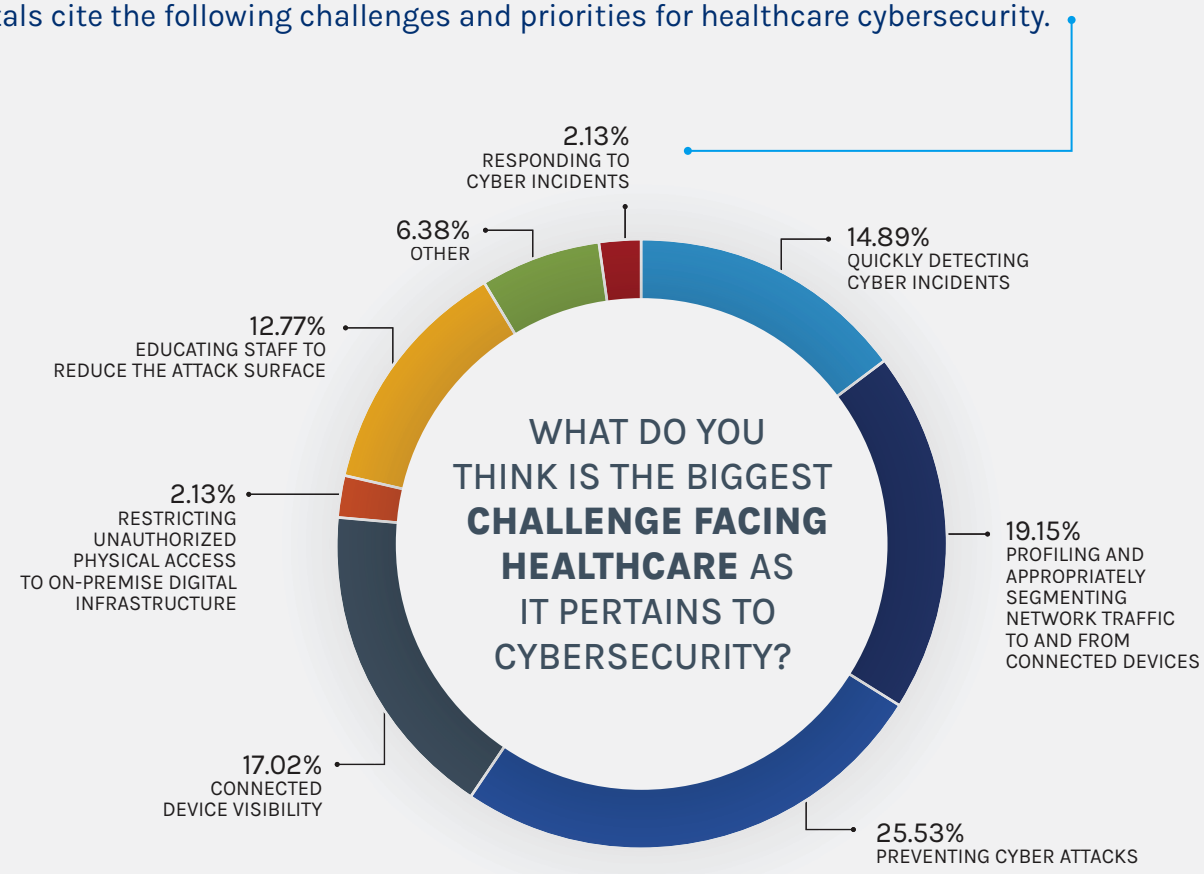
The diversity of device operating systems can make managing security increasingly challenging. When looking at the different types of operating systems found on medical VLANs, more than half (59%) were Windows operating systems and 41% were a mix of other variants, including mobile, embedded firmware and network infrastructure. Patching and updating operating systems in healthcare environments— especially acute care facilities—can be challenging and require devices to remain online and available. Some medical devices cannot be patched, may require vendor approval or need patches to be manually implemented.



SECURITY CHALLENGES AND PRIORITIES

- Most connected medical devices have an estimated useful life of 7-10 years.[11]
- With approximately 2,250 connected medical devices deployed in the average US hospital, and each device averaging an effective lifespan of roughly 8.5 years, on a yearly basis a statistically average US hospital will have around 265 devices that need near-term end of product life monitoring and planning.
- On average, it takes healthcare organizations 79 days between the time a breach occurs to the time when it is finally discovered.[2]

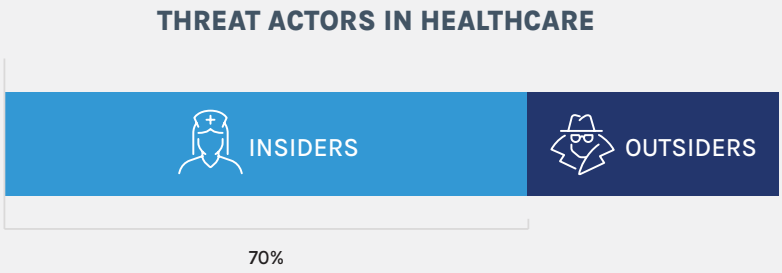
Hospitals cite the following challenges and priorities for healthcare cybersecurity.



[11] Biomedical Engineering Advisory Group; Life span of Biomedical Devices

WHAT CAN WE DO BETTER?

Healthcare is the only industry in which cyber harm is more often inflicted by insiders than outside actors — with internal misconduct (intentional or accidental) accounting for 70% of all incidents.[13]



- Breaking down those insider threats, it turns out that 47% of healthcare providers believe that employees don't understand the sensitivity and confidentiality of data they share over email.[6]
- Only 32% of healthcare delivery organizations are prepared to prevent and respond to insider threats.[6]
- And we're not doing nearly enough to change that. One of the most effective ways to manage the insider threat in through security awareness training programs, which are organization-wide efforts to engage, train and secure your employees about cybersecurity risk.
- Surprisingly, 25% of healthcare organizations say their organization has no budget for security awareness training programs this year.[14]
- 15% say that lack of budget is the most significant challenge to building and/or maintaining a security awareness training program.[14]
- Perhaps most concerning is the fact that 5% of healthcare organizations reported that their organizations have NO security awareness training programs in place whatsoever.[14] A program whose aim is to educate staff and of which the staff is unaware, cannot be very effective. The fact that respondents even see this as a possibility is a powerful indictment of an administration's perceived attitude towards dealing with issues of cybersecurity.

32%
of healthcare delivery organizations are prepared to prevent and respond to insider threats

25%
of healthcare organizations say their organization has no budget for security awareness training programs this year

15%
say that lack of budget is the most significant challenge to building and/or maintaining a security awareness training program

[13] Verizon; Data Breach Investigations Report

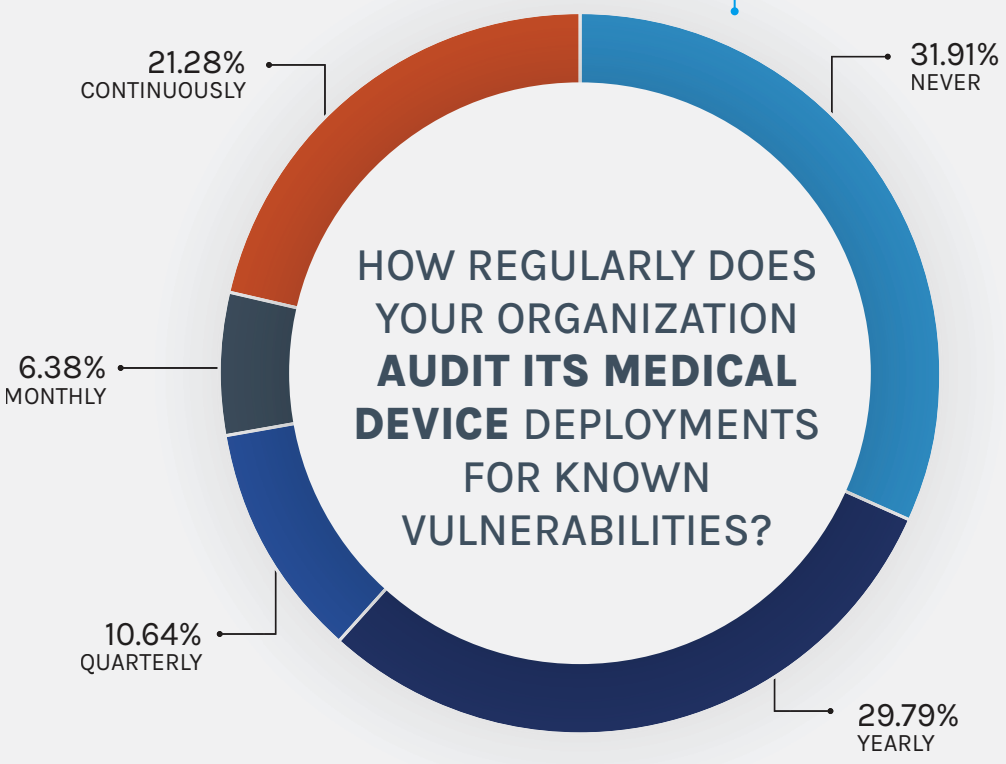
[14] SANS; 2023 Security Awareness Report

- 53% of HDOs believe medical devices are vulnerable and consider them a top cyber-attack target.[4]

- Patient ID/tracking, infusion pumps, patient monitors make up 16% of all connected medical devices.

- 96% of hospitals in the U.S. claim they were using assets with end-of-life operating systems or software with known vulnerabilities, inclusive of medical devices.[16]

Research shows that 32% of healthcare organizations never perform vulnerability audits on medical devices.



[16] Department of Health and Human Services; Hospital Cyber Resiliency Initiative: Landscape Analysis, Apr. 2023

- The healthcare industry spends 6% or less of the total IT budget on cybersecurity needs.[6]
- At the same time, there is some hope that this gap will be closed, with 58% of healthcare organizations planning to increase cybersecurity spending.[6]
- Still, 32% of healthcare organizations do not regularly brief its Board of Directors regarding cybersecurity risk, which could negatively impact their ability to allocate budget accordingly.[6]

We found an even split of organizations maintaining a devoted position of CISO and those who delegate CISO responsibilities to the likes of CIOs and IT heads. This offers support to the notion that the industry is still not treating cyber threats with appropriate seriousness.

THE COST OF DOING NOTHING

- Healthcare data breaches cost an average $10.93M, which is over 2X the cross-industry average.[22]
- On average, data breaches in the US are twice as costly as data breaches occurring elsewhere.[22]

53% of hospitals see cybersecurity as the single greatest challenge to healthcare organizations going forward; ahead of even business and profit management challenges.

NOW IS THE TIME TO ACT

The forces of digitization and connectivity bring with them tremendous potential, but they also open the door to a plethora of operational, IT, and cybersecurity challenges. With the healthcare industry in a state of prolonged disruption, the stakes are very high and likely to increase.

For hackers, healthcare represents the most lucrative industry to target and also one of the easiest. If you can hold medical equipment hostage in a ransomware attack, with lives on the line, hospital decision makers may have little choice but to acquiesce to your demands. If you don't have a taste for brutal extortion, you can turn a quick profit by punching your way into an underprotected, undersegmented network and collecting a ton of ePHI to flip on the dark web.

Any healthcare delivery organization that is not actively managing and monitoring these devices is exposed.

Imprudently managed connected devices expose the industry's soft underbelly — inviting attack. In the US alone, there are around 184 million connected medical devices spread across 6,120 hospitals. Each and every one of those devices represents a potential point of attack for the hungry hacker. That means thousands of devices that need to be actively managed and monitored to prevent breaches.

The implications of that are, in principle, daunting, and in practice, devastating; they entail continuous review of configuration practices, segmentation, network restrictions, appropriate use, credential management, vulnerability monitoring, patching & updating, lifecycle management, recall tracking, access and role controls, compliance assurance, pen testing, live context-aware traffic monitoring & analysis, oversight of partner and third-party security practices, and more.

Most healthcare delivery organizations struggle to keep track of their already managed connected devices. When you add in the typically 30-40% that are not managed or known, the potential attack vectors become significantly more difficult to mitigate. After all, how can you protect what you don't know is there?

[22] IBM; How much would a data breach cost your business? IBM; Cost of a data breach 2023 Report

CASE STUDY

The hospital recognized the need for a security and visibility management platform for the clinical assets used throughout the organization. They were lacking insight into the number of deployed devices, both managed and unmanaged, challenged with the existing manual and error-prone process for device inventory. The biomedical and clinical teams also wanted a solution that provided real-time visibility into the network that would enable them to prioritize remediation and receive alerts when a device was at risk. This hospital network was looking for one platform that could be used by multiple departments: Clinical Engineering, Security, and IT.

By more clearly defining lifecycle-wide security responsibilities and expectations with your vendors, by restricting functionally unnecessary in-VLAN communications, by investing in staff-wide cyber training, by normalizing basic network hygiene practices (like password and access management, patching & updating, etc.), and by tweaking security policies (at the NAC or firewall level) specifically for monitors, infusion pumps, and patient tracking devices, you can dramatically shrink your attack surface in short order.

Cyber attacks in healthcare are more frequent and more costly than in any other industry. The cybersecurity of hospitals, however, goes beyond the bounty price of the hacker community. Unlike any other industry, it directly impacts the well-being of the very people who are trusting the health delivery organization with their lives. Ultimately, it speaks to the core of their mission to effectively and reliably deliver a high quality of care. That's precisely why conscientious professionals and executives will want to have all the facts at their disposal. We sincerely hope that this factbook in some small way helped provide a new insight. For more information, we stand ready to help.

ABOUT FORESCOUT

Forescout Technologies, Inc., a global cybersecurity leader, continuously identifies, protects and helps ensure the compliance of all managed and unmanaged cyber assets – IT, IoT, IoMT and OT. For more than 25 years, Fortune 100 organizations and government agencies have trusted Forescout to provide vendor-agnostic, automated cybersecurity at scale.

Forecout 4D Platform™ delivers comprehensive capabilities for network security, risk and exposure management, and threat detection and response. With seamless context sharing and workflow orchestration via ecosystem partners, it enables customers to more effectively manage cyber risk and mitigate threats.an IOT security leader dedicated to protecting the quality care of health delivery worldwide.

FORESCOUT®

Forescout Technologies, Inc.
Toll-Free (US) 1-866-377-8771
Tel (Intl) +1-408-213-3191
Support +1-708-237-6591
Learn more at Forescout.com