RUNSAFE SECURITY

RunSafe Security's 2025 MEDICAL DEVICE Cybersecurity Index

Findings Report

Cybersecurity is now a primary driver of procurement decisions, vendor trust, and patient safety initiatives for healthcare executives.

RunSafeSecurity.com

Table of Contents

Executive Summary

Although cyberattacks leading to healthcare data breaches, which affected nearly 84% of the U.S. population in 2024, continue to garner the majority of the spotlight, cyber threats that breach, alter, or interfere with use of connected medical devices are a growing concern among healthcare organizations as they can impact patient care in significant and even more deadly ways.

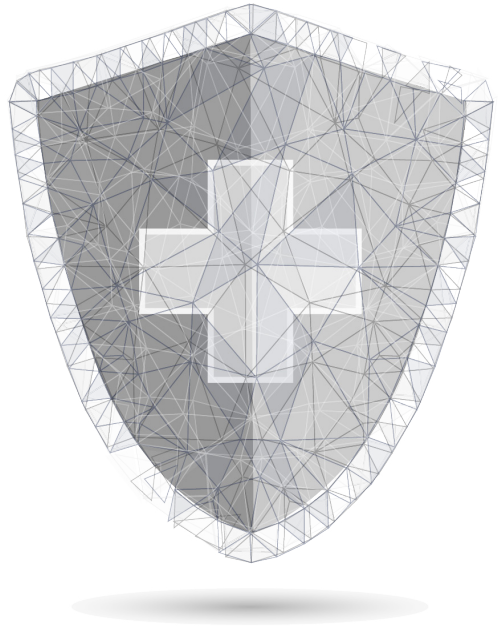
As hospitals digitize and interconnect everything from infusion pumps to imaging systems, cyber risks are no longer confined to back-office IT. Medical devices have become critical attack surfaces, and healthcare leaders are responding by placing more emphasis on cybersecurity when purchasing medical devices.

In fact, RunSafe Security's **2025 Medical Device Cybersecurity Index** reveals a sharp pivot: cybersecurity is now a primary driver of procurement decisions, vendor trust, and patient safety initiatives.

In a survey of 605 healthcare executives across the U.S., UK, and Germany involved in medical device purchasing and familiar with organizational cybersecurity protocols, the data shows:

- **22%** of healthcare organizations have experienced cyberattacks that impacted medical devices, with 75% of these incidents affecting patient care
- **35%** now identify operational technology systems like medical devices as their biggest cybersecurity concern
- **75%** of organizations increased their medical device and operational technology security budgets over the past 12 months
- **79%** are willing to pay a premium for devices with advanced runtime protection or built-in exploit prevention
- **46%** have declined medical device purchases due to cybersecurity concerns

This report outlines how cybersecurity has transitioned from the server room to the operating room — and what it means for both healthcare providers and medical device manufacturers.



Introduction

The attack surface in healthcare has expanded. Once limited to hospital networks, electronic health records, and clinical information systems, cyber threats now reach deep into the hardware and software that support direct patient care. Ventilators, monitoring devices, diagnostic tools — all are increasingly connected, vulnerable, and under threat.

Healthcare facilities and hospitals are dealing with a growing number of cybersecurity concerns as IT-OT environments converge. The FBI's Cyber Division recently reported that **53% of networked medical devices have at least one known critical vulnerability.** The Bureau's latest Internet Crime Report also stated that healthcare experienced more cyber threats in 2024 than any other critical infrastructure industry.

With this in mind, it's no surprise that the House Energy & Commerce Subcommittee recently held a hearing on the national security risks posed by legacy devices that could be exploited, with potentially deadly consequences. Experts testified that "a bad actor who discovers a vulnerability could disable patient monitors during surgeries, spoof vital signs in intensive care units, or hijack infusion pumps to administer incorrect dosages."

These vulnerabilities certainly aren't hypothetical. They've led to significant recalls and safety alerts in recent years:

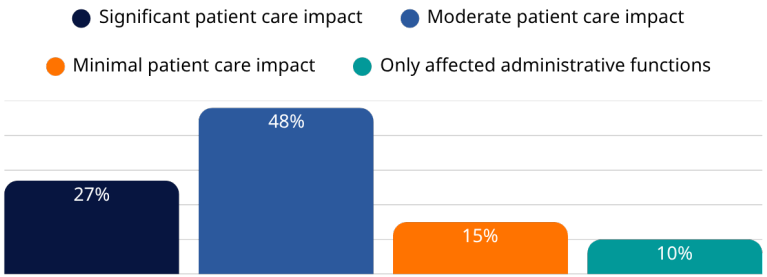
- The **2017 WannaCry ransomware attack** infected 1,200 diagnostic devices globally and forced five UK hospital emergency departments to close and divert patients.
- Also in 2017, vulnerabilities in **St. Jude (now Abbott) pacemakers and defibrillators could allow attackers to** deplete batteries or alter pacing.
- In 2019, **Medtronic insulin pumps** were recalled due to remote access risks that could let hackers alter insulin dosages.
- In 2023, **CISA and FDA** identified vulnerabilities in Contec patient monitors that could allow attackers to crash devices and steal patient data.

To better understand how this shift is reshaping the healthcare ecosystem, RunSafe Security commissioned an independent survey in May 2025 targeting decision-makers across hospitals and healthcare organizations in the U.S., UK, and Germany. All respondents play a role in medical device purchasing and are familiar with cybersecurity practices in their organizations.

This report distills the most important insights from that data to reveal how procurement processes, budget priorities, and frontline patient care are adapting to the cybersecurity imperative.

Cyberattacks Are Impacting Medical Devices and Impeding Patient Care

What was the impact of this cyberattack incident that impacted medical devices in your facility?



The theoretical risks of medical device cybersecurity have become a stark reality for healthcare organizations across the United States and Europe. Our findings reveal that 22% of healthcare organizations have experienced medical devices being compromised by cyberattacks or exploited vulnerabilities, resulting in significant consequences for patient care and operational continuity.

Among organizations that experienced cybersecurity incidents affecting medical devices, the impacts were far from minor disruptions:

- **75% of healthcare organizations say that cyber incidents have caused at least a moderate patient care impact**
- **46% required manual processes to maintain operations**
- **44% reported delayed diagnoses or procedures**
- **44% had extended patient stays**
- **24% required patient transfers to other facilities**

The fact that nearly half of the affected organizations had to revert to manual processes highlights how dependent modern healthcare has become on connected systems. Moreover, with almost a quarter requiring patient transfers, it demonstrates the severity of these incidents and their potential to cascade beyond individual facilities.

Of course, when cyber attacks cause downtime, the decision to transfer patients is often the difference between life and death. Of those that had medical devices compromised:

- **43% experienced 1-4 hours of downtime**
- **31% faced 5-12 hours without critical systems**
- **19% dealt with downtime exceeding 13 hours**
- **7% experienced more than 3 days of device unavailability**

These extended outages force healthcare providers into crisis mode, requiring backup procedures that may be less accurate, more time-consuming, and potentially compromise the quality of care patients receive.

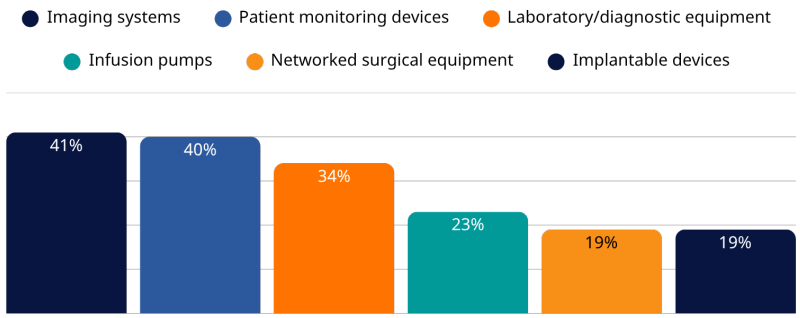
Takeaway: Even if medical devices are not the point of breach, they are being hindered by cybersecurity attacks. Healthcare organizations can no longer treat medical device cybersecurity as a future concern. These attacks are disrupting patient care today and forcing providers to make life-or-death decisions about transferring patients when critical systems fail.

Data Reveals Most Vulnerable Healthcare Systems

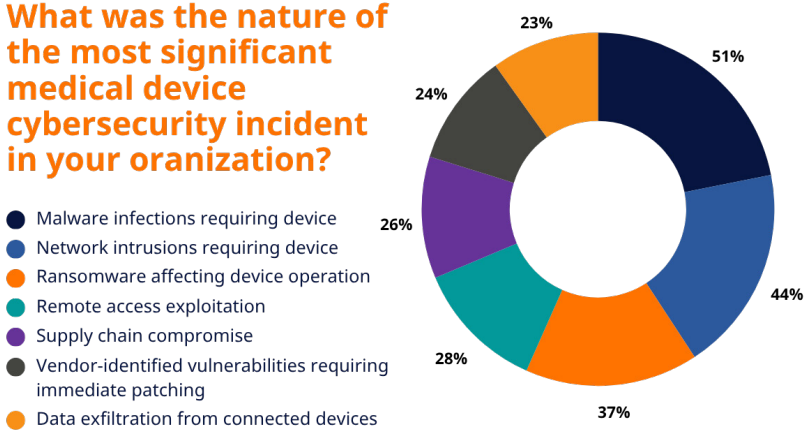
The survey data reveals a troubling pattern: cybercriminals are successfully targeting the very systems healthcare providers depend on most for patient diagnosis, treatment, and monitoring. While electronic health records systems experienced the highest rate of compromise at 52%, many cyber attackers have moved beyond data theft to operational disruption. This includes the direct targeting of critical medical devices that come into contact with patients and sustain life.

Indeed, these incidents demonstrate sophisticated targeting of mission-critical infrastructure. When a patient monitoring device fails in an ICU or an infusion pump stops working during chemotherapy treatment, the consequences are immediate and potentially fatal. In other words, attackers understand healthcare's operational vulnerabilities and are exploiting them for maximum impact.

What types of medical devices were affected by any cybersecurity incident(s)?



What was the nature of the most significant medical device cybersecurity incident in your oranization?



As for how cybercriminals are targeting medical infrastructure, malware infections (51%) and network intrusions (44%) are the primary weapons, forcing healthcare organizations to quarantine critical devices and isolate entire systems from their networks. More than a third of organizations experienced ransomware specifically designed to disrupt device operations, turning patient care into a hostage situation where lives hang in the balance of ransom payments.

The 26% rate of supply chain compromises is also concerning, as these attacks can affect multiple healthcare organizations simultaneously and are often harder to detect until widespread damage has occurred.

Takeaway: Cybercriminals are shifting from opportunistic attacks to systematically targeting the medical devices that patients rely on for life-sustaining care, compelling healthcare leaders to acknowledge that operational technology security is now a patient safety imperative.

Budgets Are Rising, But Confidence Still Lags

Healthcare organizations are responding to the medical device cybersecurity crisis with their wallets, but not with confidence. While 75% of organizations increased their medical device and operational technology security budgets over the past 12 months, only 17% feel extremely confident in their ability to detect and contain attacks on medical devices.

The fact that three-quarters of organizations opened their purse strings in a notoriously cost-conscious industry demonstrates the urgency healthcare leaders feel. 30% of all rural hospitals in the U.S. are currently at risk of closure, meaning that for many facilities, a single cyber attack could be financially devastating.

But the gap between spending and confidence suggests that simply throwing money at the problem isn't enough. This discrepancy likely stems from applying traditional IT security thinking to OT environments. Medical devices operate under different constraints than typical IT systems – they often can't be easily patched, may run on legacy operating systems, and require 24/7 availability for patient care.

This creates a critical need for runtime exploit prevention, or the ability to protect devices even when patches can't be immediately applied, and transparency into software through a Software Bill of Materials. It also calls for medical device manufacturers to integrate security features as a baseline rather than adding them as an afterthought. Which brings us to our next findings.

Takeaway: Healthcare organizations recognize the threat to their OT environments and are investing accordingly, but current security approaches aren't delivering the confidence levels needed to protect patient-critical systems. This gap is driving buyers to demand built-in security from manufacturers rather than relying on post-deployment fixes.

Cybersecurity Is Now a Procurement Prerequisite

These real-world impacts are not just reshaping incident response strategies — they're now rewriting the rules of procurement itself. In fact, the procurement landscape for medical devices has fundamentally shifted, with cybersecurity requirements now serving as a mandatory checkpoint rather than an optional consideration:

- **83% of healthcare organizations now integrate cybersecurity standards directly into their RFPs**
- **38% include detailed security requirements (not just basic checkboxes)**
- **46% have declined to purchase medical devices due to cybersecurity concerns**

This willingness to walk away from purchases represents a dramatic departure from traditional procurement practices, where functionality and cost dominated decision-making. When nearly half of potential buyers are prepared to reject products over security issues, cybersecurity has clearly transcended technical considerations to become a business-critical requirement.

This new reality is also reshaping vendor relationships. Nearly a third (32%) of healthcare organizations surveyed say security incidents have not only affected their trust in specific vendors, but they also now require additional security verification from previously trusted vendors.

Healthcare organizations are essentially conducting security audits of their entire vendor ecosystem, reassessing partnerships through the lens of cybersecurity risk rather than traditional performance metrics. And the regulatory landscape is amplifying this trend.

73% of healthcare organizations report that new FDA cybersecurity guidance and EU cybersecurity regulations are already influencing their procurement decisions. Since March 2023, the FDA's Section 524B has mandated the inclusion of cybersecurity information in submissions for network-capable "cyber devices," followed by comprehensive updated guidance in September 2023. Similarly, the EU's Cyber Resilience Act took effect in December 2024, imposing mandatory cybersecurity requirements on connected products, while the NIS2 Directive explicitly targets medium-to-large medical device manufacturers with cybersecurity compliance requirements.

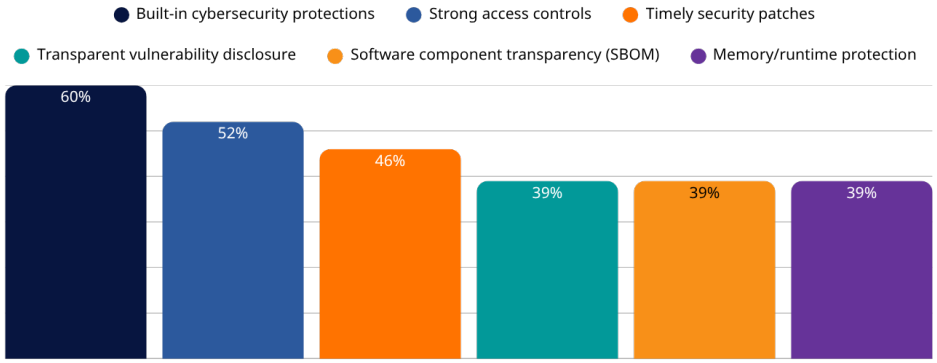
This regulatory pressure creates a cascading effect where compliance requirements drive purchasing behavior, making cybersecurity not just a competitive advantage but a regulatory necessity for market access.

Takeaway: Vendors without built-in protections risk disqualification. Cybersecurity has become a gatekeeper to market access, with procurement processes now serving as the first line of defense against vulnerable devices entering healthcare environments.

Healthcare Buyers Want Transparency and Built-In Defense

Healthcare organizations are also shining a spotlight on what cybersecurity capabilities they expect from vendors. The data reveals a clear preference for proactive, built-in security measures rather than reactive, bolt-on solutions.

Which of the following cybersecurity features influence your selection of a medical device vendor?



Most telling is that 60% now prioritize built-in cybersecurity protections when selecting vendors, signaling a fundamental shift away from devices that treat security as an afterthought. This preference reflects hard-learned lessons from cybersecurity incidents where retrofitted security measures proved insufficient against sophisticated attacks. Healthcare buyers are essentially demanding that security be baked into the device's DNA rather than applied as a surface coating.

Transparency through Software Bills of Materials (SBOMs) is also emerging as a critical requirement. 78% of organizations consider SBOMs essential or important in procurement decisions. Regulatory pressure is undoubtedly contributing to this, but so is practicality. The FDA now requires SBOMs in premarket submissions for cybersecurity preparedness, but healthcare buyers also recognize that understanding software components is fundamental to ongoing vulnerability management.

However, generating comprehensive and accurate SBOMs is a challenge for many embedded medical devices, which are often written in C/C++. Traditional binary analysis SBOM solutions produce high numbers of false positives and miss key components, like static libraries. Healthcare organizations are increasingly seeking vendors who can provide build-time SBOM solutions that accurately capture only the components actually present in the final device, streamlining vulnerability identification and response.

Runtime protection technologies are also gaining traction, though adoption remains in early stages. While 36% of organizations actively seek devices with runtime protections, another 38% are aware of these technologies but don't yet require them.

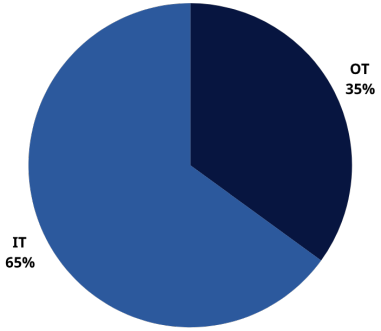
Takeaway: Healthcare buyers are demanding transparency through SBOMs and resilience through built-in protections. These requirements are rapidly evolving from competitive differentiators to baseline expectations, creating a new standard for what constitutes an acceptable medical device in the cybersecurity era.

78%

of organizations consider **SBOMs essential or important** in procurement decisions.

Operational Technology (OT) Risks Are in Focus

Are you more concerned about cybersecurity vulnerabilities within your organization's IT or OT?



As the traditional boundaries between IT and OT continue to blur, it's causing a shift in security mindset. While 65% of healthcare organizations remain more concerned about IT vulnerabilities, 35% now identify OT systems like connected medical devices as their biggest cybersecurity concern.

Real-world attacks are likely driving these concerns. As highlighted at the top of this report, a worrying 22% of healthcare organizations have already experienced cyberattacks that have impacted medical devices. But the interconnected nature of modern healthcare networks means IT and OT vulnerabilities are no longer isolated risks. Medical devices are increasingly operating on the same networks as traditional IT systems, sharing data with electronic health records, and connecting to hospital Wi-Fi networks. This convergence creates new attack pathways that allow cybercriminals to exploit traditional IT vulnerabilities, such as compromised email systems or network credentials, and gain access to medical devices.

The 2017 WannaCry attack is a perfect example of this. WannaCry spread through network connections using the "EternalBlue" exploit that targeted a vulnerability in Microsoft Windows systems. The ransomware used lateral movement techniques to spread from infected IT systems to connected medical devices. Additionally, a 2021 ransomware attack on the IT systems of Ireland's Health Service Executive (HSE), also disrupted radiology systems nationwide, forcing staff to cancel CT scans and other critical imaging procedures.

This interconnectedness means that even a successful phishing attack on a hospital employee's laptop can provide attackers with network access, enabling them to discover and target connected infusion pumps, patient monitors, and other critical devices.

Takeaway: The convergence of IT and OT security is putting medical devices at the center of cybersecurity strategy. Healthcare organizations can no longer protect medical devices in isolation. Securing patient-critical systems now requires defending the entire interconnected ecosystem.

Buyers Willing to Pay a Premium for Enhanced Protection

79% of healthcare buyers would pay a premium for devices with advanced runtime protection or built-in exploit prevention.

The convergence of regulatory pressures and real-world attacks has led to healthcare organizations demonstrating a strong willingness to invest in advanced security. An overwhelming 79% of healthcare buyers would pay a premium for devices with advanced runtime protection or built-in exploit prevention. 41% are willing to pay up to 15% more for enhanced security, while 13% would pay even more than that.

Would you consider paying a premium for medical devices with advanced runtime protection or built-in exploit prevention?

Buyers clearly recognize the real investment required for sophisticated security capabilities. In fact, only 12% of organizations expect these advanced protections to be provided at no additional cost. This suggests healthcare leaders have moved beyond viewing cybersecurity as a checkbox requirement to understanding it as a complex, resource-intensive discipline that requires ongoing investment in research, development, and implementation.

They also likely understand the repercussions of not investing: the documented financial impact of cyberattacks like WannaCry, which cost the NHS £92 million; regulatory requirements that can block market access entirely; and the recognition that cybersecurity failures can directly endanger patient lives. Healthcare organizations are essentially conducting risk-based purchasing decisions, weighing the cost of advanced security features against the potential catastrophic consequences of device vulnerabilities.

Takeaway: With healthcare buyers willing to pay premium prices for enhanced security features, medical device manufacturers now have the economic foundation to invest more heavily in security innovation, ultimately raising the baseline security standards across the industry.

RUNSAFE SECURITY

ABOUT RUNSAFE SECURITY, INC.

RunSafe Security protects embedded software across critical infrastructure, delivering automated vulnerability identification and software hardening from build-time to runtime to defend the software supply chain and critical systems without compromising performance or requiring code rewrites. The RunSafe Security Platform includes the authoritative build-time SBOM generator for embedded systems and C/C++ projects, automated vulnerability identification and risk quantification, patented memory relocation techniques to mitigate memory-based vulnerabilities, and pre-hardened open-source packages and containers for immediate protection.

Headquartered in McLean, Virginia, with an office in Huntsville, Alabama, RunSafe Security's customers span the aerospace and defense, energy, operational technology, industrial automation, transportation and automotive, medical device, and high-tech manufacturing verticals.

RunSafeSecurity.com
571.441.5076
Sales@RunSafeSecurity.com

Conclusion

Cybersecurity has evolved from an IT concern to a patient safety imperative that drives every aspect of healthcare operations. From procurement decisions that can block market access entirely to real-world attacks that force hospitals to divert ambulances and cancel surgeries, medical device security now sits at the intersection of regulatory compliance, operational continuity, and patient care.

The data shows an industry in transition, where 46% of healthcare organizations decline purchases based on security concerns, where SBOMs have become mandatory requirements rather than optional documentation, and where buyers demonstrate willingness to pay premium pricing for advanced protection.

For medical device manufacturers, this transformation presents both opportunities and imperatives. Those who embrace transparency through comprehensive SBOMs, integrate runtime protections and built-in security, and demonstrate proactive vulnerability management will find themselves positioned to capture market share in an industry increasingly willing to invest in advanced protection. Conversely, manufacturers who treat cybersecurity as an afterthought risk not just regulatory rejection, but exclusion from a market that has fundamentally redefined what constitutes an acceptable medical device.

The convergence of IT and OT security combined with unprecedented regulatory oversight and buyer sophistication has created a new competitive landscape. Cybersecurity excellence now serves as the foundation upon which trust, market access, and patient safety are built.

46%

of healthcare organizations **decline purchases** based on security concerns