SANS

How a Leading Med-Tech Organization Reaffirmed the Value of Cybersecurity Training

When the leadership team at a leading global medical device manufacturer began a company-wide review of programs and spending, every department was asked to reexamine its priorities. The goal was to streamline operations and ensure resources were focused on the initiatives most critical to innovation, patient safety, and regulatory compliance.

For the Medical Device Cybersecurity office – a specialized group responsible for securing the company's medical devices – the review presented a challenge. Training and development programs are often among the first to be scrutinized during such initiatives, and the group's management knew they would need to demonstrate not just the importance of training, but its measurable business value and return on investment.

Rather than defending cybersecurity education as a necessity, the group positioned it as a strategic advantage. The team's long-standing partnership with SANS Institute became central to that argument and a tangible example of how focused, skills-based learning had improved productivity, accelerated compliance readiness, and strengthened internal expertise.

"We knew we had to show that investing in people wasn't just the right thing to do; it was the smart thing to do.

The team gathered data on the impact of its training investments. Engineers who had completed cybersecurity courses were mentoring peers, leading threat assessments, and accelerating product security reviews. Their skills were shortening development timelines and helping ensure smoother regulatory approvals. In a heavily regulated industry where every delay carries both cost and compliance risk, those outcomes spoke volumes, not only as proof of improved performance but as tangible indicators of ROI.

As they presented the case to senior leadership, the management framed training as a financial decision as much as a technical one. Developing expertise internally was proving far more efficient – and far more sustainable – than attempting to source it externally. Hiring experienced cybersecurity professionals from outside the medical device sector required months of recruitment, onboarding, and domain acclimation, while upskilling existing engineers through targeted training kept critical expertise in-house and avoided the high cost of turnover. "When you invest in people, you keep expertise in-house," he explained. "That knowledge pays off in every design review, every audit, and every launch."

The results of that discussion were clear. The organization not only reaffirmed its commitment to ongoing cybersecurity training but strengthened its focus on scaling that capability across teams, recognizing it as a high-value investment with measurable return.

To understand why the argument resonated, it helps to look at the broader context.

Over the past decade, medical technologies have become increasingly connected. Devices that once operated in isolation now share data through wireless interfaces and cloud-based systems. That connectivity has revolutionized patient care, but it has also created new entry points for potential cyberattacks. "We're not just protecting networks or data," the management noted. "We're protecting devices that keep people alive."

Recognizing this reality early, the company established the Medical Device Cybersecurity office to embed cybersecurity into every stage of product design and development. The team brought together engineers, clinicians, and

HOW A LEADING MED-TECH ORGANIZATION REAFFIRMED THE VALUE OF CYBERSECURITY TRAINING

security specialists to ensure new products were both safe and secure by design. But as the field of connected healthcare evolved, so too did the complexity of threats. Many engineers were experts in medical technology but less experienced with modern security frameworks, while professionals hired from IT security backgrounds often lacked familiarity with the clinical and regulatory environment.

To close that gap, the company expanded its collaboration with SANS Institute to provide practical, hands-on training. Participants began with foundational courses in network defense, threat modeling, and secure software development, followed by advanced modules in areas like mobile and web application security. "The labs made it click," the management recalled. "You could immediately see how the concepts applied to what we build every day."

The impact was tangible. Engineers could identify and mitigate risks earlier in development, reducing rework and preventing costly delays in product approval. As regulations around medical device cybersecurity became more stringent, that competence proved invaluable. "Our products can't move forward without meeting cybersecurity expectations," they said. "When developers understand security, we save time, reduce rework, and ultimately protect patients."

Today, the Medical Device Cybersecurity office is seen not as an operational expense but as a growth enabler. The organization's training investments continue to yield measurable ROI from improved retention, product innovation, stronger regulatory confidence, and faster time-to-market. "Our success depends on how fast our people can adapt," the management reflected.

"SANS gives them the tools to do that. It's not just cybersecurity training; it's business enablement.