Fortified HEALTH SECURITY

Middlesex Health's Incremental Cybersecurity Strategy

Increasing risks, decreasing resources

After a phishing attack in 2015, Middlesex Health's Chief Technology Officer (CTO) and Chief Information Security Officer (CISO), Dave Christiano, worked with the executive team and board to put more robust safeguards in place.

In addition to needing healthcare-specific cybersecurity expertise, Middlesex's IT team also required 24/7 coverage capabilities.

"Staffing and budget constraints is a challenge many of us face in healthcare IT. One of the things that exacerbate both of these issues is having enough staff to provide night and weekend support, which is essential if you're going to run a 24/7/365 security program," explains Christiano. "After our breach, we were shuffling people from the day shift to nights, and outsourcing support to staff our help desk for nights and weekends. But that wasn't a viable long-term solution."

The phishing attack also raised awareness throughout the organization about the precarious financial situation that a breach puts the health system in.

"We're very fortunate that many individuals on our board come from industries where cybersecurity is highly prioritized," shares Christiano. "When I presented my recommendations for an incremental approach to increasing our cybersecurity resources, and how that would be cost-effective for Middlesex, they responded with support and enthusiasm for our plan."

Middlesex Health

Health System:
Middlesex Health

Location:
Middletown, CT

Number of Locations:
127

Website:
https://middlesexhealth.org

Strategic cybersecurity support

Christiano and his team had previously contracted with Fortified Health Security to conduct their HIPAA-based NIST risk assessment.

> "Our initial engagement with Fortified exceeded expectations," reflects Christiano. "They went beyond just conducting a comprehensive risk assessment. Their ongoing engagement included regular monthly calls, monthly scans of our entire network, remediation recommendations, and a mitigation plan for addressing these issues both efficiently and cost-effectively. Without these measures in place, the impact of the breach would have been far more severe. I firmly believe that it was their expert guidance that enabled us to successfully manage and swiftly resolve the cyber attack."

After the breach, Christiano knew from first-hand experience that Fortified would be the right managed security services provider (MSSP) to guide them along their cybersecurity maturity path.

"After our risk assessment and going through the phishing attack with Fortified, we knew it was critical to add on Vulnerability Threat Management (VTM). From there, we progressed with Incident Response Services, followed by Managed Endpoint Detection & Response (Managed EDR), and Managed Connected Medical Device Security (IoMT) monitoring," shares Christiano. "For us, these were foundational services that we needed to not only get our cyber program off the ground, but to holistically protect our organization and patients."

Planning and preparation

With the phishing breach still fresh in their minds, Christiano recognized the vital importance of ensuring that everyone at Middlesex Health, from the leadership to the frontline staff, was ready and equipped to respond in the event of another cyber incident. He also knew that one of the most effective ways to prepare an organization for such an ordeal is through engaging tabletop exercises.

> "I can do a lot of technical tabletops for my team and throw out various scenarios, but it's a different ball game when it comes to an executive tabletop. Having Fortified facilitate a tabletop exercise for our leadership added a level of seriousness and expertise that was more impactful than if it had been conducted by our internal team," says Christiano. "I can't wait to do our next one because it was so eye opening for everyone and led to important internal conversations, especially around how to handle downtime if we face a serious cyber incident."

> Integrating 24/7 Managed EDR and IoMT services greatly simplified our staffing issues and streamlined operations. Surprisingly, it also positively impacted our bottom line," shares Christiano. "The combined cost of these services is actually lower than what we were spending on five full-time employees to manage the same tasks during off-hours."

Integrating 24/7 protection

For Christiano, it was also important to have a healthcare cybersecurity partner providing 24/7 Managed EDR services services who also had a foundational understanding of their cyber program, people, and established processes.

"I've heard so many stories of cybersecurity vendors parachuting in, only to be limited in their ability to help because they have no baseline for what happened before they got there. Not having that context actually slows down the resolution process. It's far more effective to be proactively prepared with a trusted partner who's familiar with your environment," says Christiano.

Middlesex's security team, while highly committed and experienced, is often stretched thin due to their demanding workload. Partnering with Fortified has given them an extra set of skilled hands to promptly tackle alerts and tasks that might otherwise be delayed. This collaboration not only supports a manageable workload but also plays a crucial role in preventing burnout among the team.

Positive progress and peace of mind

Partnering with Fortified has bolstered the confidence and preparedness of Christiano and his team as they navigate the ever-evolving threat landscape.

"While it's an ongoing process, I know we're in a better place organizationally when it comes to cybersecurity," said Christiano. "I love it when the Fortified team presents a hypothetical disaster scenario on our monthly calls because it's fantastic to hear how adept my team has gotten with their response strategies."

Among his peer group of hospital CIOs and CTOs, Christiano is often asked what he's doing to establish such a strong cybersecurity program for Middlesex.

"I could not be more passionate about telling them that we've found an incredible MSSP partner that offers the whole gamut of cybersecurity services specifically designed for healthcare, and who goes above and beyond to ensure we're a happy customer," says Christiano. "Year after year, Fortified's expertise has streamlined our cybersecurity efforts, reduced our operational expenses, and eased our stress. I have no doubt my team and I are sleeping better at night because we're better prepared, and have the right systems, processes, and people in place."