El Camino Health: Human-focused Security Strategy Heralds New Patient Safety Era of Cybersecurity

The health system's unique approach and its cybersecurity partner ensure clinical and business continuity

Founded nearly 70 years ago, El Camino Health (ECH) provides Northern California's Silicon Valley and South Bay communities with nationally recognized clinical care at two not-for-profit hospitals in Los Gatos and Mountain View, physician clinics and urgent care locations across the region. Today, the health system maintains 466 hospital beds with 1,552 physicians and serves nearly 300,000 patients yearly. It consistently garners patient-care accolades: ECH has been named one of Newsweek's "World's Best Hospitals" in 2024, a Most Wired Hospital in 2024 and is ranked among the nation's top hospitals for maternity and cardiac care.

But when it comes to cybersecurity, the system requires a dedicated focus upon continuous improvement in which the work is never complete, with ongoing assessments providing valuable next steps. Call it "strategic humility." "We focus on what's next and what's left to accomplish," said CIO Deborah Muro.

Muro's thoughtful approach to cybersecurity has not gone unnoticed by her colleagues. She was recognized with a 2024 Bay Area CIO ORBIE in the large enterprise category, an award presented to chief information officers who have demonstrated technology leadership excellence. According to Ryan Witt, Chair of Proofpoint's Healthcare Customer Advisory Board, Muro is a leading light in the industry because she understands that cybersecurity is entering a new era that connects security to a healthcare system's foremost mission: ensuring the safety, healing and well-being of every patient.

"In the last couple of years, there's been a big shift in healthcare's mentality towards cybersecurity and the importance of a cyber posture," Witt said. "Many systems had treated cybersecurity as a kind of insurance, with compliance and box-checking. These are still factors in risk calculation, but there's a much stronger calculation that El Camino uses: will exposure create patient safety risk? Therefore, do I need to make investments in technology, people and processes to mitigate against that exposure?"

"As threats have grown, we realized we must have a partner who's going to help with them."

DEBORAH MURO | CIO | El Camino Health

A human-centric cybersecurity strategy

Muro acknowledges that her human-centric approach has been a continuous work in progress and credits partnerships with industry leaders for its development. "You cannot take care of your business without having a partner like Proofpoint," she said. "Proofpoint provides a protection layer between the user and the attacker in the email scenario especially. As threats have grown, we realized we must have a partner who's going to help with them. And we've been adding more functionality as it becomes available."

The human-centric cybersecurity strategy stratifies threats by using real-time intelligence to identify an organization's most likely attackers and most-likely-to-be-attacked personnel. Muro says that ECH leans on Proofpoint as a security partner to provide information on current malicious actors, whether they are lone wolves, criminal syndicates or nation-state actors. The system also incorporates the latest intelligence on exploits, scams and schemes, as well as those specific people and departments who are being targeted within the organization.

"I'm a data-driven person," Muro said. "I prefer data-rich information, and users appreciate the level of specificity provided by this platform. It helps everyone understand the layers of defense against malicious exploits and, at the same time, educates frequently attacked individuals to remain on high guard."

This approach contrasts with a "moats and walls" strategy that applies the same level of resources and expense to every possible attack. Not only does this burn finite resources on largely improbable or non-existent threats, but it fails to focus on the most likely attackers, victims and targets of attacks.

"There are still organizations that need to get the basic blocking and tackling of security in place," Witt said. "But institutions like El Camino are making investments in the controls needed to search for the proverbial needle in the haystack. It is a very nuanced capability to solve for a smaller use case — the kind in which a highly targeted, highly specific attack evades traditional defenses and can be catastrophic if it is not prevented."

An ounce of prevention

According to the *2024 Verizon Data Breach Investigation Report*, nearly 7 in 10 breaches resulted from a non-malicious user falling prey to a social engineering attack or making an error in judgment.[1] So, Muro directs significant effort and resources to equip healthcare professionals and staff with the skills to develop lasting security practices and promote positive behavioral changes.

"How can technology prevent a malicious email from arriving in an unsuspecting individual's inbox?" Muro asks. It's a bit of a trick question, because while it focuses attention on "technology" and an incoming email, Muro's starting point is to reduce the number of potentially "unsuspecting" individuals. ECH's IT security team uses existing use case scenarios and exercises to craft an ongoing prevention program to educate its users. The key is constant vigilance, assessment and intervention.

"We want to make sure that the correct way to deal with a certain scenario is widely known," Muro explained. "We make sure we educate people beforehand, and then we send out a test to determine how well they understood that information and how well they're adhering to the protocol or the procedure."

And when someone doesn't follow the procedure, or if someone fails an exercise, Muro's team then compares its in-house data to Proofpoint-provided industry benchmarks to identify weaknesses and redirects its education and remediation efforts accordingly.

"Proofpoint has been able to help us look at that [data] and put a good strategy together for current state and then to where we want to go in the future, to keep elevating our protections and our security," she said.

Current state, future state

The speed at which future states become current state is a challenge for healthcare CIOs. New cybersecurity tools need swift evaluation and implementation to defend against ever-evolving attacks.

"We want to make sure that the correct way to deal with a certain scenario is widely known."

DEBORAH MURO

"This is the beginning of the new patient safety era of cybersecurity, where executive teams see a direct connection between a cyber event and adverse patient outcomes."

RYAN WITT | Chair, Healthcare Customer Advisory Board | Proofpoint

One such attack is impersonation, a growing threat vector that targets organizations' service and help desks. Sophisticated hackers, drawing on content from social media, the dark web and institutional web pages, are using email and even phone calls to impersonate clinicians and non-clinical staff. If the organization's ID procedures aren't strict enough, the hacker can gain credentials that allow them to access the organization's IT systems.

"The industry is seeing more and more of these social engineering attacks," Witt said. "And CISOs and CIOs need intelligent tools to help their teams stay a step ahead."

Muro believes that tools enhanced with artificial intelligence (AI) can level the playing field against hackers. For example, these tools could instantly correlate data about senders, recipients and message content to help users assess the legitimacy of every email that arrives in their inboxes. It could even quarantine emails that fail an AI inspection.

She is also challenging Proofpoint to help her manage a growing portfolio of third-party applications. "Every third party brought into an organization adds to the exposure risk, which grows exponentially with each new application," Muro pointed out. "You need to ask if the benefits of a new application outweigh the third-party risk."

ECH is developing a third-party risk program to prospectively evaluate new applications while retrospectively analyzing the existing portfolio. With the 2024 Change Healthcare breach still fresh in everyone's mind, the program will also identify beneficial redundancies so that if access to a third-party application is interrupted, its continuity plan ensures normal operations.

"Getting the organization to proactively invest in redundancy is important before you're in a disaster," Muro said. "If you wait until an event to figure it out, that's too late."

Witt said that ECH's leadership is heartening. "This is the beginning of the new patient safety era of cybersecurity, where executive teams see a direct connection between a cyber event and adverse patient outcomes," he noted. "They understand that any cyber event has the potential to disrupt a procedure or the ability to receive a new patient, or to force a hospital to transfer patients to another facility — or even in the most drastic instance, impact mortality."

Witt concluded, "It's not about brand value, financial compliance, regulatory, et cetera. It's a fundamental shift in the risk calculation, and its day has come."

To learn more, visit proofpoint.com/healthcare.

Reference

1. Verizon. 2024. *Verizon 2024 Data Breach Investigations Report*. https://www.verizon.com/business/resources/reports/dbir/.

proofpoint

About Proofpoint

Proofpoint, Inc. is a leading cybersecurity and compliance company that protects organizations' greatest assets and biggest risks: their people. With an integrated suite of cloud-based solutions, Proofpoint helps companies around the world stop targeted threats, safeguard their data, and make their users more resilient against cyber attacks. Leading organizations of all sizes, including 85 percent of the Fortune 100, rely on Proofpoint for human-centric security and compliance solutions that mitigate their most critical risks across email, the cloud, social media, and the web. More information is available at www.proofpoint.com.

Produced by HIMSS