CASE STUDY

PREVENTING RANSOMWARE AND OTHER THREATS AT HALIFAX HEALTH

The Florida healthcare system invested heavily in email security and end-user training

With his board's backing, Halifax Health Vice President and Chief Information Officer Tom Stafford embarked on an expansion of cybersecurity operations at the 92-year-old community hospital system based in Daytona Beach, Florida. Among his top priorities: preventing both ransomware that locked down critical systems, and data heists accomplished through fraudulent email.

Both types of malicious activity were on the rise nationally. And they still are. Data breaches are becoming more commonplace and ransomware is forcing hospitals to divert patients to other facilities until the malware can be removed or the ransom paid in cryptocurrency. Stafford wanted to devote enough resources to mitigate those risks as much as possible and keep Halifax Health out of the headlines.

That put enormous pressure on Stafford's cybersecurity and incident-response staff. The organization's portfolio includes a 600-bed medical center that treats 136,000 patients annually and two other smaller hospitals, including one that opened in February 2020. In addition, Halifax Health provides ambulatory, urgent care, home health, and hospice services for Volusia and Flagler counties' residents.

"Our organization is the steward of our patients' data, and as soon as patients come to us, they are entrusting us to protect that data," Stafford explained. "I've made proper purchases to strengthen ourselves to a point where we have a greater chance of protecting our patients' information."

"Our organization is the steward of our patients' data, and as soon as patients come to us, they are entrusting us to protect that data."

Tom Stafford | Vice President and Chief Information Officer | Halifax Health

Chief among those purchases: a solution to specifically detect and deflect email-borne attacks that surreptitiously unleash malicious code and cripple clinical operations—usually using spear phishing. According to Trend Micro, 91% of targeted cyber attacks today originate with email, making it a priority among cyber protections. Stafford needed a way for his team to quickly flag suspicious emails in both real time and around the clock. He also needed a way to educate everyone working at or for Halifax Health on how to spot phishing expeditions before they could do damage.

Solution priorities: Industry reputation and ease of use

"We chose Proofpoint Email Security and Protection because Proofpoint has a great reputation in the industry and because of its ease of use for both us and our employees," Stafford said.

The solution allowed Halifax Health to set up strong filtering policies and detailed firewall rules to better manage inbound emails. That preventative tool is augmented by ongoing threat intelligence, which is gathered from all Proofpoint customers and analyzed by machine-learning algorithms. This allows Halifax Health to stay up to date with the latest ploys from email imposters.

Also, the Proofpoint email security platform includes Targeted Attack Protection (TAP). TAP continuously monitors Halifax Health accounts for suspicious emails and then alerts the team to active threats. This helps Halifax Health IT security team members avoid alert fatigue and devote more time to promptly responding to incidents or other duties. And just as important to Stafford is ongoing awareness training and testing to build a well-educated user base capable of spotting something potentially malicious. And, should training fail, there's a mechanism to prevent malicious attachments or embedded URLs from opening on Halifax Health mail servers.

HALIFAX HEALTH

"That's probably one of the biggest benefits of Proofpoint: It's always flagging suspicious emails and preventing them from getting through to us," Stafford noted. "It also serves as a deterrent in that if someone does open an attachment in an email because he or she trusts that email, that attachment is actually opened up in Proofpoint's cloud. So, if that attachment is malicious, Proofpoint prevents it from ever getting downloaded to our environment."

The chances of that happening are growing slimmer as Stafford's team continues to train users, from top executives to entry-level employees, to recognize the latest threats or phishing scams—both at work and at home. "Making the training relevant outside the office helps to ensure that

> ***"Cybersecurity is a challenge. But Proofpoint enables us to see who the bad actors are, and has a tool to filter out a lot of emails that come through from lists."***
>
> **Tom Stafford** | Vice President and Chief Information Officer | Halifax Health

users better retain concepts and recommended countermeasures," Stafford said. Here again, Proofpoint provides cloud-based training modules and regularly scheduled phishing simulations to boost user awareness and gauge workforce compliance.

User awareness training is working, according to Stafford. Halifax Health now has an extremely low malicious-link click rate of 1% to 2% among its 4,000 employees. But, as he quickly noted, "It only takes one person to click on the wrong link to have a disastrous event."

While anyone can fall for a phishing scam, some job functions attract more attacks than others–people with prized data or access, such as pharmacists, or clinicians involved in publicized research. "We call them internet celebrities—those most likely to be attacked because they are all over the internet," he said. "And I'm one of them."

By cobbling together information culled from public sources and social media, cyber criminals can build a convincing narrative to launch a credible email attack. That makes those with broad digital footprints bigger targets for email fraud, since they interact regularly with the public and are more likely to receive emails from unknown and untrusted sources.

Greater transparency, insight and protection

"Cybersecurity is a challenge," Stafford admitted. "But Proofpoint enables us to see who the bad actors are, and has a tool to filter out a lot of emails that come through from lists. We can now more easily create whitelists for our users."

Stafford's team has established multiple "deterrents"—a word he prefers to "defenses" because he knows anyone with enough determination will find a way into a system. In addition to traditional firewalls and intrusion detection tools, one of the best deterrents are end users always on guard for malware masquerading as legitimate-looking attachments or URLs embedded in emails. That's where continuous training comes in, along with the ability to report suspicious email by simply clicking on a phishing icon on their Microsoft Outlook program.

Stafford advises his healthcare administrators and IT leaders to follow cybersecurity trends and understand how bad actors target and compromise organizations. And then install as many deterrents as possible to protect that "golden data."

"Every year, we prepare for hurricanes," he said. "And every day, I have to prepare for a cyber attack."

Halifax Health, main campus | Halifax, Florida

The effects of any cyber attack—particularly ransomware—can be just as disruptive and devastating as a natural disaster for today's healthcare organizations. "Five or 10 years ago, that wouldn't have been the case; we could have more easily reverted to a paper system. But today through Meaningful Use, we've become very reliant on our electronic systems to document care. If we lose those, that's a disaster," he said.

In addition to the protections a robust email security platform provides, Stafford believes in conducting periodic penetration tests to challenge a current system. "Everyone does all this work to prevent getting attacked," he said. "But there really are only two ways to test that readiness: You can conduct pen testing, or you can do nothing and see what happens. And if I were to ever choose the latter, my title changes from Chief Information Officer to My Career is Over."