LEVERAGING CYBER RESILIENCE STRATEGIES TO BOLSTER DEFENSES AGAINST HEALTHCARE EMAIL ATTACKS

While unsettling and disruptive, email attacks are no longer surprising. According to *How U.S. Hospitals and Health Systems Approach Email Security*, a survey of 101 healthcare professionals conducted by HIMSS Media, 9 of 10 healthcare organizations experienced at least one type of email-borne threat in the past year.

"All the reasons email is useful for legitimate purposes, make it useful for malicious purposes. Ultimately, email attacks are prevalent because they work."

MATTHEW GARDINER | DIRECTOR OF ENTERPRISE SECURITY MARKETING | MIMECAST

"The stat is remarkably consistent with other industries and other surveys," said Matthew Gardiner, director of enterprise security marketing at Mimecast. "Email attacks are so prevalent because email is one of the most ubiquitous applications in the world. Pretty much any organization that an attacker is interested in has people using email. And, it's easy for an attacker to reach into an organization via email. All an attacker needs to know is someone's email address."

In addition, with email, attackers can attach files and links to websites — and deliver this suspect content right to a user's inbox, all while remaining anonymous. As such, "All the reasons email is useful for legitimate purposes, make it useful for malicious purposes. Ultimately, email attacks are prevalent because they work," Gardiner said.

Indeed, cybercriminals have embraced email attacks because they generally have a very high return on the attacker's investment and all of disruption costs fall to the victimized healthcare organization. In fact, 25% of the healthcare professionals who participated in the study reported that the email-borne attacks they experienced were either extremely or very disruptive, while another 35% said the attacks were somewhat disruptive.

Impersonation of trusted vendors or partners via email was the most frequent disruption method, with 61% of respondents characterizing the aftermath as very or extremely disruptive, followed by credential harvesting focused phishing attacks (57%), and data leaks or threats initiated by cybercriminals stealing users' log-in credentials (35%).

"We leverage a combination of training, sophisticated technology and threat intelligence to make sure the right messages get to us, and that when they don't, our teams have the tools to handle it. This layering helps make sure our systems, trading partners, and customers are as protected as possible. Email hygiene is one of our top security priorities."

TAYLOR LEHMANN | VICE PRESIDENT AND CHIEF INFORMATION SECURITY OFFICER | ATHENAHEALTH

Andrew Heins, vice president and chief information security officer at LifePoint Health, a national healthcare network, pointed out that phishing emails, when successful, can be significantly disruptive. Healthcare organizations are expected to continually mature their analysis methodology to ensure prompt and effective investigations of all reported phishing emails. In addition, response procedures require immediate action to reduce the risk exposure associated with this evolving threat.

According to Taylor Lehmann, vice president and chief information security officer at athenahealth, a healthcare technology company, the problem is that healthcare organizations can't return to normal business operations until they are certain they have completely eliminated the threat. "Once an organization's network has been penetrated, they must then spend the cycles necessary to restore operations safely and with proper security controls," Lehmann said.

Healthcare organizations, however, are fighting back. Consider the following: Nearly three-quarters of organizations have a cyber resilience plan in place or are planning to roll one out (Figure 1).

In addition, healthcare organizations have made significant investments in cybersecurity technologies. For example, 80% of survey respondents reported that their organizations have implemented firewalls/next-generation firewalls, 79% have implemented email security systems, and 78% data backup and recovery solutions. However, while many organizations have made progress, considerable risk will prevail until all organizations have fully implemented these controls (Figure 2).

Both Heins and Lehmann noted their organizations are addressing information security and email threats through layered defenses, which rely on multiple security controls, technologies, and strategies to protect against attacks.

Also embracing a layered defense, athenahealth continually strives to refine its multifaceted approach to optimally safeguard the organization. "We conduct regular data breach simulations where we bring in our responders and simulate an attack," Lehmann said. "These exercises provide our teams an opportunity to practice and build situational awareness on the state of our protections and our response capability. We learn about what areas we need to improve and that is key to make sure we have the right plans in place."

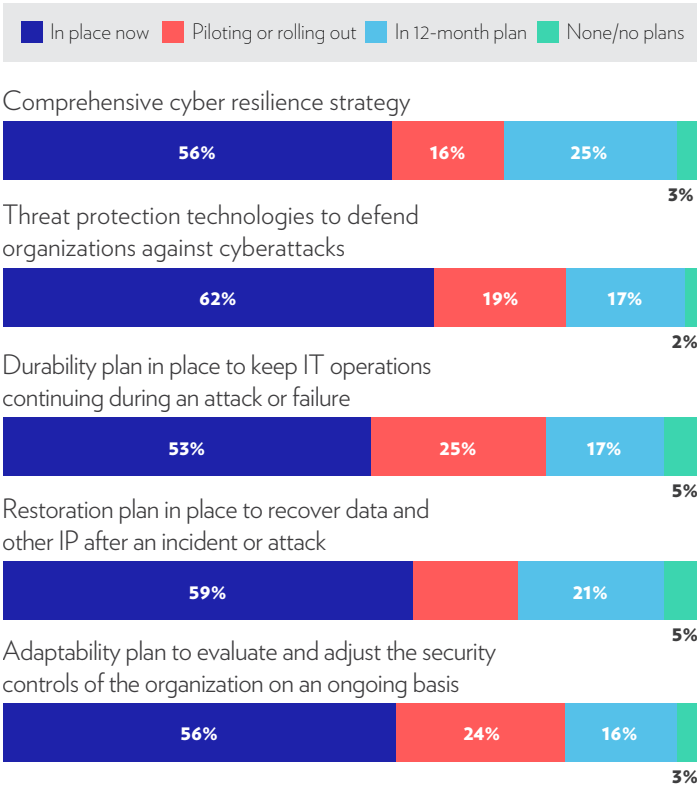
This approach has prompted athenahealth to zero in on email protection, Lehmann said. "We leverage a combination of training, sophisticated technology and threat intelligence to make sure the right messages get to us, and that when they don't, our teams have the tools to handle it. This layering helps make sure our systems, trading partners, and customers are as protected as possible. Email hygiene is one of our top security priorities."

Keeping up with threats

While healthcare organizations are addressing data security concerns, the challenge is to stay one step ahead of the bad actors.

"Many organizations have been investing in people and technology and general improvements in security, but the attackers have industrialized, specialized, and accelerated their abilities as well," Mimecast's Gardiner said. "So, while organizations have improved their defenses, threats have continued to as well, making it very difficult for organizations to sufficiently protect themselves."

Figure 1. Status of cyber resilience across entire IT program, and where surveyed leaders' organizations stand



"With this [Mimecast awareness training] service, employees can quickly review two-to-three-minute videos on various cybersecurity topics, including email safety."

ANDREW HEINS | VICE PRESIDENT AND CHIEF INFORMATION SECURITY OFFICER | LIFEPOINT HEALTH

As a result, healthcare organizations need to intensify and diversify their efforts to ensure the cyber resilience programs are working. Understanding exactly what constitutes an effective cyber resilience program is a necessary step.

"People frequently fixate just on the technologies and assume they are protected because they are using an antivirus system, a backup system, an email security system, and other tools," Gardiner said. "All of this is good. However, information technology professionals also need to think about other elements of a program."

More specifically, IT professionals should focus on creating business processes that can shield them from attacks, on optimizing security tools, and on delivering effective staff education.

"The problem is that people think, because they're implementing some aspects of cyber resilience programs, they're resilient," Gardiner noted. "However, when they operate in the real world, they find that, unfortunately, they are not as protected as they thought, and they get disrupted. So, they need to re-scrutinize their resilience program."

Employee-focused security awareness

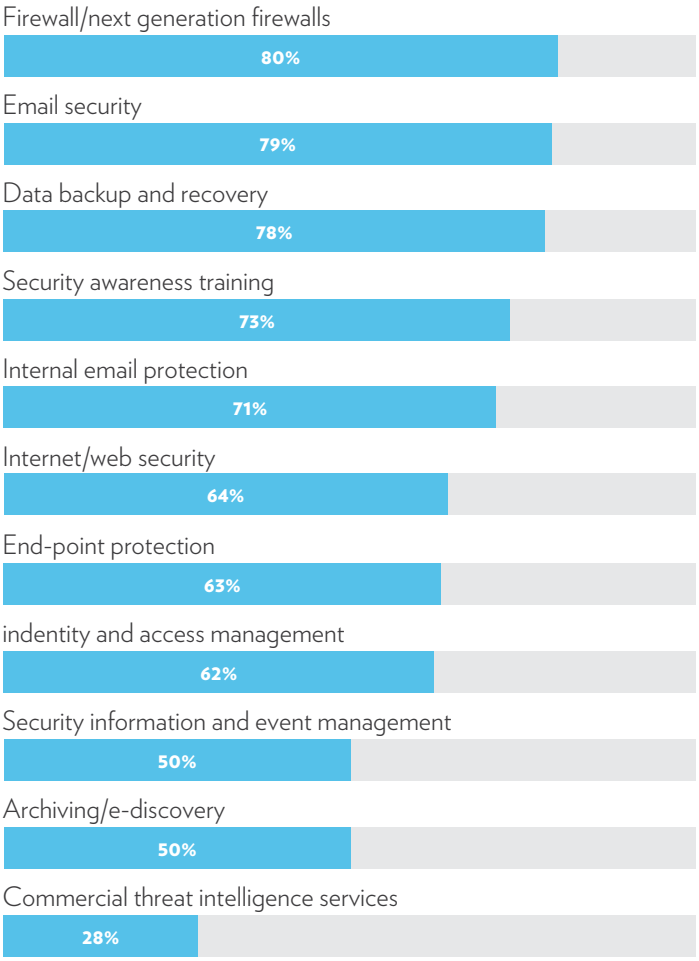
Employee training is one element of a cyber resilience program that requires significant attention. Indeed, 77% of the healthcare professionals who participated in the HIMSS Media study agreed that employee-focused security awareness is an essential component of defending against email-borne cyberattacks. Such training is important, as 69% of respondents indicated that an email outage of more than a few hours would greatly affect their organizations' ability to function. In addition, just 50% agreed cloud-based email systems (such as Office 365 or GSuite) are sufficiently secure against the multiple forms of phishing on their own.

Yet, 40% of respondents indicated that their organizations are providing security training to employees less than quarterly (Figure 3). More frequent training, however, could pay off. "Organizations are better off doing five minutes of training once a month, instead of 15 minutes of training once a quarter," Gardiner said. "Even though it's the same amount of time, it's better to do the training more often so the information stays top of mind."

In addition to offering training more frequently, healthcare organizations can also increase training effectiveness by delivering the content in an engaging format. LifePoint Health conducts monthly phishing training and is also adding additional education for its employees via a streaming platform, Heins said. "With this service, employees can quickly review two-to-three-minute videos on various cybersecurity topics, including email safety."

Lehmann added that athenahealth is striving to make its email education more effective by continuing to offer more user-friendly options.

Figure 2. Security controls now included or planned to be included in cyber resilience plans, according to respondents



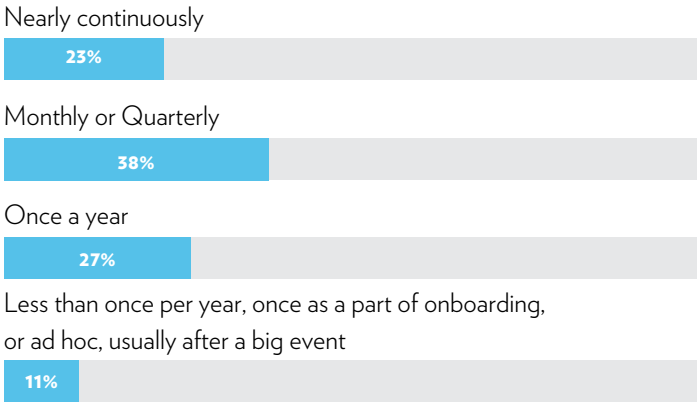
"We continue to be focused on ways to use training opportunities to encourage positive outcomes. Questions like 'how do we reward staff for doing the right thing with suspicious messages?' are our focus."

TAYLOR LEHMANN | VICE PRESIDENT AND CHIEF INFORMATION SECURITY OFFICER | ATHENAHEALTH

"Many email threat training programs focus less on learning and encouraging the right behaviors, and more on turning immediately punitive when enough failures to 'learn' occur. We continue to be focused on ways to use training opportunities to encourage positive outcomes. Questions like 'how do we reward staff for doing the right thing with suspicious messages?' are our focus," he said. "Although there may be negative impacts as a result of continued failure, we want our teams to become email threat-hunters, looking for the link or file not to click and get a positive outcome that encourages that action again and again."

By proactively addressing the effectiveness of training programs, healthcare organizations can add to the strength of their cybersecurity defenses. While it is likely not possible to reach a state of absolute security perfection, the right cyber resilience strategies, combined with effective technical security controls, can help organizations stay healthy in the overall fight.

Figure 3. Frequency of employee email training



mimecast

About Mimecast

Mimecast is a cybersecurity and compliance provider that helps thousands of organizations worldwide make email safer, restore trust and strengthen cyber resilience. Mimecast's expanded cloud suite enables organizations to implement a comprehensive cyber resilience strategy. From email and web security, archive and data protection, to awareness training, uptime assurance and more, Mimecast helps organizations stand strong in the face of cyberattacks, compliance risk, human error and technical failure. www.mimecast.com