Mimecast Research: 90 Percent of Healthcare Organizations Hit with an Email-Borne Attack in the Past Year

March 10, 2020

Report Highlights Latest U.S. Healthcare Email Security Attacks and Need for More Effective Employee Awareness Training

LEXINGTON, Mass., March 10, 2020 (GLOBE NEWSWIRE) -- Mimecast Limited (NASDAQ: MIME), a leading email and data security company, today announced the availability of a new joint research report from Mimecast and HIMSS Media, *How U.S. Hospitals and Health Systems Approach Email Security*. This research provides quantitative insights on the latest email-borne threats facing healthcare organizations. The report found a staggering 90 percent of healthcare organizations experienced an email-borne threat in the past year – with one-in-four respondents stating these attacks were very or extremely disruptive. The research also revealed that employee security awareness training is not properly prioritized within cyber resilience programs.

Healthcare organizations hold massive amounts of medical and personal information, making them lucrative targets for threat actors. While many organizations are investing in people and technology to improve cybersecurity defenses, attackers have also up-leveled their tools and tactics to evade detection and more effectively land their exploits. According to the research, the top attack types targeting healthcare organizations' email are malicious URLs and broad phishing attacks. Even though 3-in-4 organizations reported having or are in the process of rolling out a comprehensive cyber resilience program, only half of respondents disclosed high levels of confidence with their current email security deployment.

In fact, 72 percent of organizations experienced downtime as a result of an attack, with productivity (55 percent), data (34 percent) and financial (17 percent) being the three most common types of losses. Healthcare organizations experiencing the most disruptions over the course of the last 12 months were hit more frequently by attacks impersonating trusted vendors or partners (61 percent) and credential harvesting focused phishing attacks (57 percent) in comparison to other kinds of email-borne attacks.

"The popularity of email as a communications channel makes it one of the top attack vectors used to target healthcare organizations. All the reasons it is effective for legitimate use, makes it a key path for threat actors to use maliciously, often with minimal efforts and a high return on investment," said Matthew Gardiner, director of enterprise security at Mimecast. "This research puts a spotlight on the email security challenges faced by the healthcare industry. To better prepare, information technology and security professionals must strengthen their email security programs by combining the best technical controls with knowledgeable staff and resilient business processes to avoid disruption from email-borne attacks."

Additionally, employee training is a key element of a comprehensive cyber resilience program – one that is often overlooked. Seventy-seven percent of respondents agreed that employee-focused security awareness training is essential to protecting their organization against email-borne attacks, yet 40 percent indicated that their organization provides security training less than once per quarter. Shockingly, 11 percent admitted to only offering trainings during onboarding or ad hoc after a negative incident had occurred.

"Organizations are better off doing five minutes of training once a month, instead of 15 minutes of training once a quarter," said Gardiner. "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."

Cyber Resilience Think Tank member, Taylor Lehmann, who serves as the vice president and chief information security officer at athenahealth said, "Leveraging a combination of training, sophisticated technology and threat intelligence," can help strengthen an organization's cybersecurity defenses.

Read the full whitepaper based on the results of *How U.S. Hospitals and Health Systems Approach Email Security*.

Visit Mimecast's new **Threat Intelligence Hub** for more reports and research.

Methodology
HIMSS Media conducted this research in November 2019 on behalf of Mimecast. A total of 101 qualified respondents answered the survey. Qualified respondents had significant involvement with email security initiatives at U.S. hospitals and health systems. This was a blind data collection effort. Mimecast was not identified as a sponsor of the research.

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

Mimecast Social Media Resources
LinkedIn: Mimecast
Facebook: Mimecast
Twitter: @Mimecast
Blog: Cyber Resilience Insights

Press Contact
Alison Raymond Walsh

Press@Mimecast.com
617-393-7126

Investor Contact
Robert Sanders
Investors@Mimecast.com
617-393-7074

Source: Mimecast Limited