# Use Cybersecurity Awareness Month as a springboard -- not a fire drill

techtarget.com/cybersecurity/news/366651182/Use-Cybersecurity-Awareness-Month-as-a-springboard-not-a-fire-drill

Alissa Irei October 1, 2026

## National cybersecurity awareness efforts peak in October, but attacks happen year-round. Experts explain how CISOs can use Cybersecurity Awareness Month to build long-term momentum.

Every October, enterprise cybersecurity teams schedule phishing simulations, host lunch-and-learns and remind users to practice good password hygiene. Then November arrives, and -- in many organizations -- attention fades.

"By December, the [phishing] click rates are right back where they started," said Chris McGlasson, fractional CIO with ClearStack Advisory. He told TechTarget he sees this pattern unfold firsthand in many of his client organizations. "The month doesn't create vigilance; it creates a checkbox."

The U.S. Department of Homeland Security and the National Cybersecurity Alliance (NCA) started Cybersecurity Awareness Month in 2004 to help Americans stay safe online. Experts agree the month has strategic value in the enterprise -- if CISOs use it to jump-start security initiatives and generate momentum they can sustain for the rest of the year. Organizations that treat Cybersecurity Awareness Month as an annual fire drill, however, risk creating complacency rather than momentum.

"If October is the only time people hear about cybersecurity, we shouldn't be surprised when the lessons fail to stick," said Lisa Plaggemier, executive director at NCA. "The smartest approach security leaders can take is to use October as a launchpad."

## Use Cybersecurity Awareness Month to build momentum

While cyberthreats are a 24/7/365 reality, Cybersecurity Awareness Month is just 31 days long. Experts agreed that CISOs should use that window to prioritize a few changes that -- depending on an organization's security gaps -- promise the biggest bang for the buck.

With deepfake and voice-cloning attacks on the rise, for example, an enterprise might consider codifying and communicating proof-based, out-of-band verification processes. "Any request involving money or sensitive data gets confirmed through a second channel, no exceptions, even when it's 'urgent,'" McGlasson said. "Especially when it's urgent."

Other possibilities include implementing MFA, encouraging strong password hygiene and teaching users how to spot AI-enabled scams. "Then, throughout the other 11 months,

reinforce those behaviors," Plaggemier said.

Regular short training sprints beat yearly one-off marathons, agreed Kevin Walker, founder and senior cyber security consultant at Black Swan Cyber Security Solutions. Even better: ground messaging in real-world incidents and attack trends that grab users' attention.

"Talk about incidents and near-misses that have actually happened in your organization or sector," Walker said. "A five-minute conversation about a real scam affecting businesses like yours can be more useful than another annual thirty-minute training module that everybody clicks through to get the certificate."

## Measure outcomes and track year-round trends

Track security awareness levels throughout the year, experts advised, using quantitative metrics such as click-through rates on simulated phishing emails and internal incident reporting rates. With an informed sense of what works and what doesn't, CISOs can then strategically adjust training initiatives and programming in October and beyond.

Walker said CISOs at larger organizations, especially, should also keep tabs on harder-to-measure cultural indicators.

"Are people comfortable saying, I think I might have made a mistake? Are managers supporting somebody who slows a payment down because they want to verify it independently?" Walker said. "That tells you far more about your security culture than whether 98% of employees completed a module."

McGlasson compared Cybersecurity Awareness Month to New Year's resolutions, which can be ineffective and fleeting -- or spark lasting improvements. Among his client organizations, he added, those that get the most out of cybersecurity's annual spotlight use it as a catalyst for ongoing change rather than treating it as a finite event.

"One October of training buys you about 90 days of better behavior," McGlasson said. "A year-round rhythm buys you a different company."

*Alissa Irei is an Informa TechTarget news reporter covering cybersecurity.*