OVERVIEW: Despite the time, energy, and resources poured into hardware and software solutions, people remain at the heart of information security.

CHALLENGE: While a recent study found that 75% of security events come from external sources, many require internal resources – our employees – to be successful. The same study found that security breaches are nearly three times more likely to occur because of social-engineered attacks on employees. Despite these findings, adding new technologies remains the best preventive measure identified by organizations. Creating a security-minded culture does not even make the list of top strategies for most organizations.

SOLUTION: Marin County uses a combination of technology and culture to address threats. Recently, several upgrades were implemented that both improved information security and reduced costs. These included enabling security features in Microsoft Office 365 and implementing new firewall and endpoint security solutions, providing the tools necessary to proactively protect data from unauthorized access and maintain a secure infrastructure. These technologies are proven to defend against advanced malware attacks, have built in automation, analytics, and forensic capabilities, and provide advanced correlation of data for improved network visibility.

INNOVATION: In conjunction with mandatory security awareness training, the Information Security Team conducts monthly mock phishing exercises. It is an inexpensive solution that reaps significant rewards because email phishing scams are one of the top causes of security breaches. Monthly results are shared with departments, and based on these findings, several departments receive custom, in-person training for their "frequent clickers," including hands-on exercises to identify "red flags" in suspicious e-mails. Employees can also report suspected phishing e-mail messages using the "Phish Alert" button within Office 365. County employees love the instant feedback they receive when "catching" the mock phishing email. A pop-up message congratulates them! It reinforces their diligence.

The County celebrates National Cyber Security Awareness Month in October with brown-bag security awareness sessions and other activities. Our next initiative is to roll out a security ambassador in each department; further embedding information security into the fabric of the organization.

RESULTS: Upgrading security technology resulted in an annual savings of $240,000. The mock phishing exercises demonstrate that employees are becoming more educated, with several departments achieving zero clickers in monthly campaigns. Employees have become more aware of the cyber threat landscape and are incorporating security best practices into their work.

REPLICABILITY: Including information security as an organizational priority, requiring annual security awareness training, and conducting monthly mock phishing exercises and targeted training are inexpensive best practices that can be implemented by other California counties.

PROJECT OR PROGRAM CONTACT: Jason Balderama, Chief Information Security Officer, County of Marin, 1600 Los Gamos Dr., Suite 370, San Rafael, CA 94903, jbalderama@marincounty.org, 415.473.7827