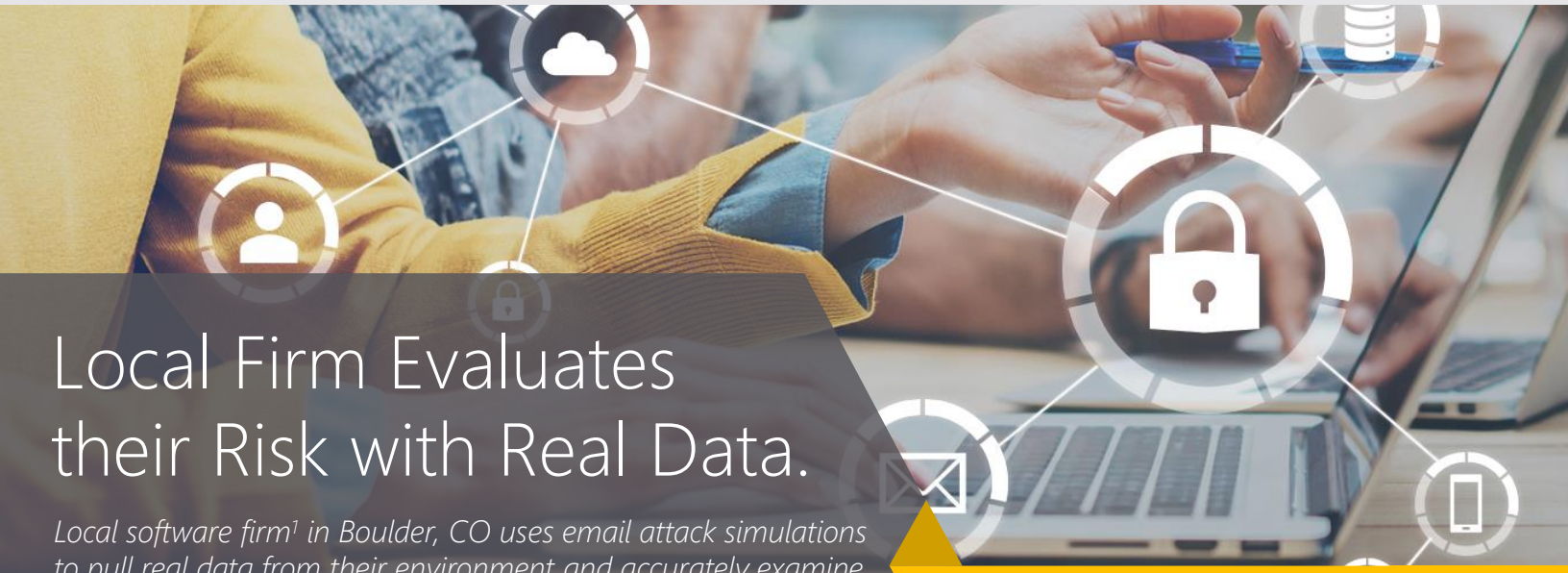
PEI

www.pei.com | 303-786-7474 | info@pei.com



Local Firm Evaluates their Risk with Real Data.

Local software firm[1] in Boulder, CO uses email attack simulations to pull real data from their environment and accurately examine the security risk of their 40-person user base.

The Challenge

Your users are your greatest asset, but they can also be easy targets for introducing vulnerabilities to your environment through the fastest-growing attack vector: email.

Phishing email attacks increased 250%[2] in 2018 and continue to grow in both number and sophistication.

When deciding where to allocate security funds, this software firm felt their status as a tech company meant users were ready to spurn potential phishing attacks. Were they right?

Our Strategy

This local firm wanted to get the most out of their limited security budget, so PEI ran a security assessment and phishing simulation to identify the most pressing vulnerabilities in their environment.

- PEI sent out a simulated phishing email including a few key suspicious details—like misleading links and a mismatched domain.
- We collected data on how many users clicked on the suspicious link and entered their work credentials when prompted.
- This provided the firm with real data that could be analyzed to provide insights for prioritizing specific security initiatives.

The Results

SOFTWARE FIRM USES REAL DATA TO PRIORITIZE PRESSING SECURITY CONCERNS.

SEVENTY PERCENT. of users clicked on the suspicious link. Clicking on a link can take users to malicious sites or launch malware.

THIRTY PERCENT. of users entered their work credentials, even though the link specified it led to a third-party site.

EIGHT USERS. who entered their credentials had admin access to the firm's IT environment. Just one slip gives malicious actors complete access to your business.

The firm identified user awareness and training as a primary security need and achieved leadership buy-in for the initiative. PEI then helped implement a custom plan for routinely educating and testing users.

1. Customer has asked not to be named in this report due to the nature of the findings.
2. Microsoft Security Intelligence Report. Volume 24, 2018.