networks whether they are in the office, working offsite or on vacation in another country. At the same time, data breaches are growing in complexity and sophistication.

Apr. 14, 2017

In today's digital environment, employees are connected continuously to enterprise networks whether they are in the office, working offsite or on vacation in another country. At the same time, data breaches are growing in complexity and sophistication. As a result, data breaches are no longer confined to just the IT department, but are now affecting every department within an organization. More importantly, each breach leaves a lingering, if not lasting, imprint on an enterprise's brand.

Because there are a lot of similarities in different types of data breach scenarios, Verizon has opened up the cyber case files in our second annual Data Breach Digest (DBD) so that industries can strengthen their network security processes. The DBD details 16 real-world data breach scenarios based on their prevalence and/or lethality in the field. It is important for organizations to understand how to identify signs of a data breach and important sources of evidence so they can investigate, contain and recover from a breach as fast as possible.

Given today's highly charged cybercrime environment, CPAs can play a vital role in helping their clients become aware of commonly used tactics to better protect financial assets. It's important to understand that timing is critical when it comes to incident response. The reality is, cybercriminals can break in and steal data in a matter of minutes. In 93 percent of scenarios we examined where data was stolen, we found that systems were compromised in minutes or less; actual data exfiltration happened within minutes in 28 percent of the scenarios. But even where exfiltration took days, the criminals didn't need to worry as in 83 percent of cases, victims didn't

find out they had been breached for weeks or more. The longer it takes an

trips. After every trip, the "travel" devices were wiped and rebuilt. This practice simplified the process of isolating any potential breaches.

In this scenario, Verizon's investigative team found that the CSO's smartphone and laptop had been subject to malicious activity, but further analysis revealed that the issues occurring on the two travel devices were likely unrelated. Fortunately, both appeared to have been subject to opportunistic compromises rather than targeted threats. Both devices were then re-imaged to their baseline builds and file system artifacts were loaded into the company's security monitoring platforms to determine if other devices had been affected.

Based on this specific incident, CPAs are in a position to recommend the following strategic tactics to help their customers better protect against social engineering (phishing) scams and other data breach attempts:

- Require two-factor authentication for access to email from the Internet.
- Require Virtual Private Network (VPN) access for telecommuter and travellers accessing company networks.
- Encourage travellers to note travel device usage times, locations, and other details including connections and accounts used.
- Train employees required to travel on proper device and data handling while out of the office; provide resources related to country-specific legal concerns prior to travel overseas.
- Limit administrative access for employees to their devices; if admin access is required for job function, enact a policy restricting use or installation of non-approved third-party apps.
- If possible, provide employees with travel devices that can be rebuilt upon return; limit access from these devices and keep known baselines to expedite digital forensic review.

CPAs need to remind customers that awareness is the first and best line of defense

companies adopt new technology.

For more information, the complete Data Breach Digest can be downloaded here.

# # #

Firm Management • Security • Technology