

To Stop Data Breaches, Prioritize Employee Education

The work of learning leaders may revolve around building organizational knowledge and skill development crucial to company success, but new research shows few are educating employees around smaller, seemingly innocuous behaviors that can have costly implications.

According to Verizon's [2015 Data Breach Investigations Report](#), an organization's employees account for more than 50 percent of its data breaches. Sadly, it's no wonder, considering 35 percent of enterprise employees don't think data security is their responsibility, and 60 percent can't distinguish between confidential and nonconfidential files, though 70 percent of employees do have access to and use confidential company files — according to [research](#) conducted by security software developer CoSoSys.

Anything like an employee opening up an email attachment from a suspicious sender, downloading an unapproved application for a convenient work-around, or unknowingly sharing private company information with an outsider can open up the door for trouble. Some of the more well-known data breaches — of companies like the NSA, Target and Sony — are believed to have been caused by insiders, and the fallout adds up whether the compromised business is big or small. Verizon calculated an expected cost of \$254 per record for breaches involving 100 records, meaning close to half a million dollars for 100,000 records lost.

To reduce their vulnerabilities, ITProPortal.com, a U.K.-based IT resource website, suggests companies create customized data security training for employees. Data security behaviors aren't one-size-fits-all because different employees do different work.

“The content must be rendered effective by simplifying and tailoring it to the employee being taught so that they understand clearly what is at stake, and feel confident they understand what needs to be done to protect themselves and the company,” ITProPortal.com reported.

Bravetta Hassell is a Chief Learning Officer associate editor. Comment below or mail editor@CLOmedia.com