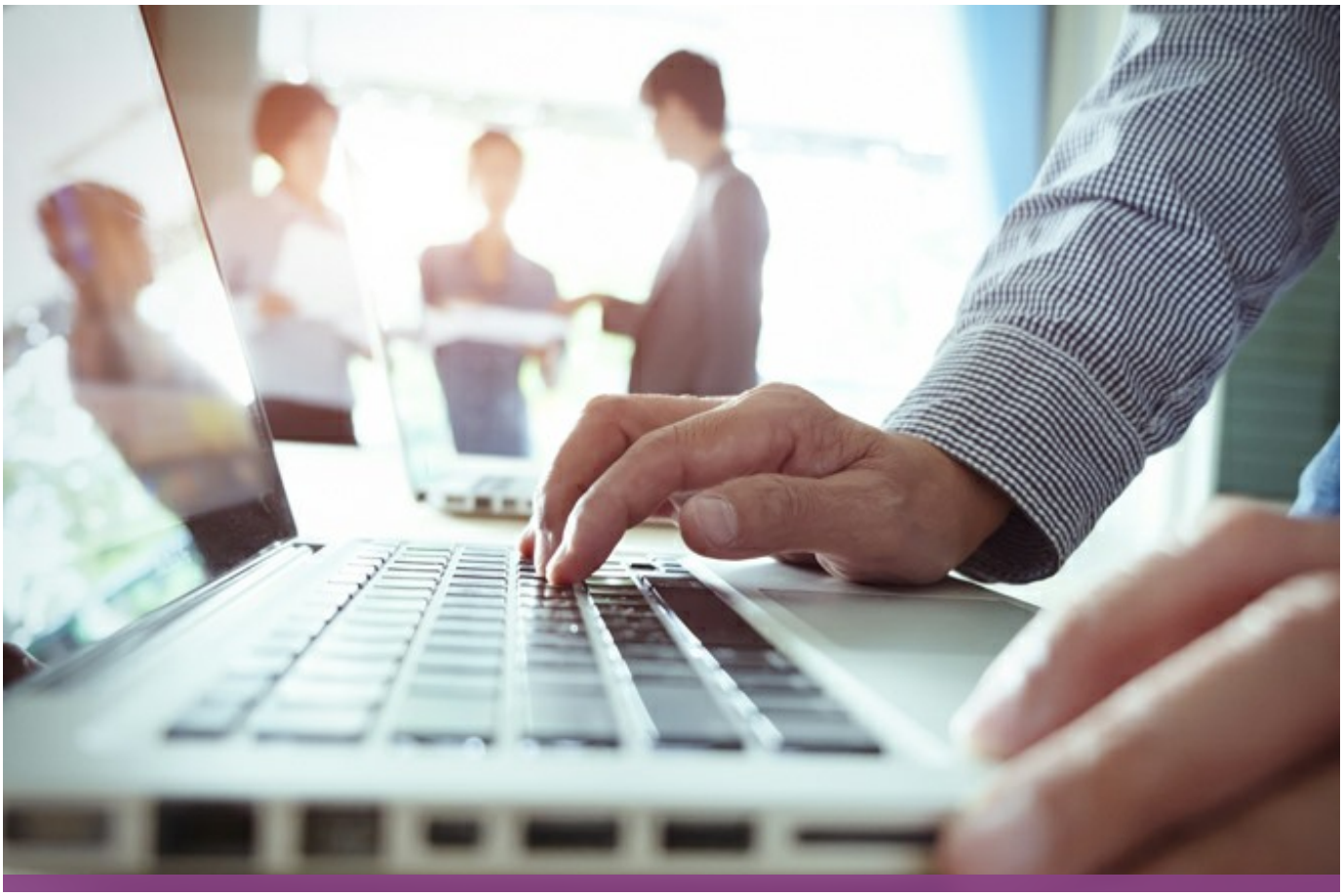
Best practices for data privacy and cybersecurity employee awareness training



James J. Giszczak, Dominic A. Paluzzi, Miriam L. Rosen | Wednesday, March 7, 2018

Have you added data privacy and cybersecurity employee awareness training to your 2018 training matrix? When it comes to data privacy and cybersecurity, employees can be your greatest asset and your greatest weakness.

Frequently, the human element (i.e., human error) is the cause of data breaches. In 2017, companies experienced an epidemic level of employees making mistakes – from sending files of personal and financial information (sometimes including W2s) to threat actors who sent phishing emails posing as an executive, to falling victim to email phishing scams that allow someone access to their entire inbox. While most employers provide onboarding training to new employees and some training throughout the year, it is best practice to train all employees on cybersecurity and data privacy awareness. In addition, employers should provide more in-depth training if the employee handles sensitive data in their position.

EMPLOYEE TRAINING BEST PRACTICES

To limit or avoid human error with data privacy and information security breaches, training should occur at all stages of employment.

- **Onboarding.** All new employees should receive data privacy and information security awareness training on the organization's data privacy and security polices and procedures, including, for example, how to respond to email requests for sensitive and/or financial information and how to store information (full encryption of devices and portable storage). Employees also need to be trained on how to respond to emails that appear to come from the C-suite. One type of email that employees frequently receive and erroneously respond to is an email that appears to come from an executive requesting employee personal or financial information. Employees must be trained to recognize such emails and how to properly respond. This includes training that it is best practice to call and speak with the supposed requestor prior to emailing sensitive data, especially if the request appears out of character for the requestor.
- **Position specific.** Employees in certain positions and departments or employees who handle sensitive

data (payroll, finance, human resources) should receive specialized training. Policies and procedures should include the minimum access principle; individuals are given minimum access to sensitive data necessary to perform a job or task and the access is granted for the minimum time necessary.

- **Tabletop exercises and phishing training.** Organizations should include practical training, including tabletop exercises and simulated exercises to determine how well employees respond to data privacy and information security crises. Further, phishing programs train users how to identify and avoid or properly respond to phishing emails.
- **Annual training.** All organizations should provide annual retraining on their data privacy and information security policies and procedures, awareness training, and position specific training. Records of all data privacy and cyber security training and retraining should be maintained and may be requested by a regulator conducting an audit or investigation.

POLICES AND PROCEDURES ALL EMPLOYERS SHOULD HAVE IN PLACE

It is also a best practice for employers to have certain policies, agreements and training in place related to data privacy and cybersecurity. A few of the policies that all organizations should have in place include:

- Written Information Security Program
- Incident response plan
- Computer and electronic device usage policies

State and federal regulators investigating data breaches often consider whether the organization maintains appropriate data privacy and cybersecurity policies, agreements, and training to protect the organization. Importantly, if the organization has a first and then subsequent data breach and does not have such policies in place, the regulator may consider that a factor in finding liability for the data breach.

For questions related to employee training on data privacy and cybersecurity, or to have a risk assessment conducted to determine which policies, agreements and training are right for you, contact one of the McDonald Hopkins attorneys listed below.

James J. Giszczak

Dominic A. Paluzzi

Miriam L. Rosen