THE
NATIONAL LAW REVIEW

The Importance of Cybersecurity Training

Friday, October 12, 2018

Article By Murtha Cullina
Daniel J. Kagan Newsletters and Alerts

Communications, Media & Internet
All Federal

According to Verizon's 2018 Data Breach Investigations Report, phishing or other forms of social engineering cause 93% of all data breaches. In order for phishing or social engineering attacks to be successful, the attacker needs a target to take the bait. Your employees often are the targets, aka the fish that bite. Therefore, in conjunction with the implementation of IT security measures, training your employees is of paramount importance to preventing these types of cybersecurity attacks. Employers must make employees aware of the risks associated with clicking on a link in a phishing email, downloading an attachment from an unknown sender or responding to requests for credential/login information or other data.

Employee training is one of the least expensive and most effective tools an organization can use to reduce the risk of a cyberattack. This training can be both formal and informal. Formal training would include training on your organization's policies and procedures as well as specific incident response training. For informal training, organizations should consider periodic e-blasts to employees detailing current threats and simulated phishing attacks with follow-up feedback. For example, e-blasts could include reminders that: (1) during the holiday season they are likely to see phishing emails that purport to be from UPS or FedEx, requiring a user to click a link related to a package; and (2) employees should never provide log-in credentials when requested via email even if the email appears to be legitimate. Also, organizations should consider providing payroll staff an annual refresher on the increased likelihood of a W2 phishing scam in December, January and February. During this time period, payroll staff are most likely to receive an email, purportedly from the CEO or CFO, requesting all employee W2 information. Overall, these types of reminders are a great way to ensure that cybersecurity stays on the forefront of your employees' minds in between more formal training sessions.

Practical training methods should not stop with an organization's general workforce. In addition to the employee training described above, companies should consider engaging in tabletop exercises that prepare an organization to react in the unfortunate event it experiences a breach. Specifically, these exercises simulate a data breach incident and allow an organization's executives to test the organization's ability to respond in the event of an attack using its formal policies and procedures. Overall, through frequent exposure and regular training, your organization will develop a culture of cybersecurity awareness.

Lastly, as indicated in our launch of Cybersecurity Awareness Month, we would be remiss if we did not note that the Department of Homeland Security created a Toolkit to provide companies with resources to promote the importance of cybersecurity awareness.

Source URL: https://www.natlawreview.com/article/importance-cybersecurity-training