CEP Magazine - August 2023

Dian Zhang (dian.zhang@gartner.com) is Research, Senior Principal at Gartner in Arlington, Virginia, USA.

How to develop relevant, applicable cybersecurity training

By Dian Zhang

Data breaches are dangerous and costly. Human errors—such as opening an email from an unknown source, giving away passwords to an insecure website, or sharing proprietary information with an artificial intelligence chatbot—can often be the culprit.

When trying to orient busy employees to secure behaviors with relevant and applicable training, compliance must do these three things:

Segment employees by needs

Not all employees need the same training. To group people by risk exposure, work with information security, human resources, business unit heads, and managers to map out each team’s responsibilities and access to crucial business information. Then identify the potential risks each group may generate and plan for training courses on suitable topics.

Next, quiz each employee on their cybersecurity knowledge to further understand the depth of content you should provide. For instance, if one team displays insufficient understanding compared to others in the same area, deploy more training to close the gaps.