Top Tips for Developing Effective
Security Awareness and Training Programs

A common saying is that an organization's employees are the weakest link in information security. While there is some truth to that statement, employees should be viewed as part of the solution, not the problem. Information security awareness and training activities can provide some of the best return on investment. If implemented properly, the organization's leadership will see fewer instances of employees falling prey to cyber threats and tactics, such as social engineering, and greater reporting of suspected attempts to compromise the organization's critical assets. To implement and maintain an effective information security awareness and training program, several "best practices" and building blocks should be used.

Leadership

Senior leadership involvement in awareness and training activities is a critical aspect of any awareness and training program. Leadership involvement sets the tone for the program and supports the message that information security is vital to the business' goals and objectives.

Resources

Awareness and training activities can be conducted without a large outlay of monetary resources, yet those activities can have a significant positive impact in the organization's overall defense-in-depth strategy. In addition, awareness and training activities do not need to take up a large amount of employees' or trainers' time.

Learning

Depending on the size of the organization, there may be up to five generations of learners, and each generation, in general, learns differently. Within the learning model, activities for employees generally fall into the awareness and training categories. To enhance retention of the information provided, consider activities that take into account the various generations of learners. Gaming and challenges are popular across all generations, so consider adding them into the mix.

Strategy

To have the most effectiveness, a long-term strategy should be developed to provide leadership's vision of the culture it hopes to instill. To support the strategy, a 2-year plan detailing quarterly information security themes and topics should be developed. Activities can then be based on these themes and topics.

Analytics

To ensure there is a proper balance of activities and information, metrics can be useful. First, to understand the organization's current culture, a "baseline" should be developed. From this baseline, other metrics collection and analysis methods can be used to gauge whether the organization's security culture is shifting in the direction envisioned in the strategy.

Persistence

Information security training conducted one time per year is simply not enough. Awareness and training activities should be spread across the year to provide greater persistence. Cyber threats are constantly changing, and the awareness and training program must be agile enough to provide information regarding the latest threats.

Timeliness

Information provided to employees should reflect the latest news about best security practices, cyber threats, and company information security policies and standards. Information provided to employees in a timely manner may mean the difference between avoiding a data breach or falling prey to an attack that causes significant damage to the business.

Relevance

Awareness and training activities should include not only information relevant to work and the business, but information that applies to employees at home and on travel. As organizations see more business conducted on personal devices, as well as the impact of cybercrime on employees in home and travel settings, the awareness and training program should provide information pertinent to these situations.

Feedback

One of the best "bang for the buck" training activities is sending your organization's employees phishing emails, simulating social engineering tactics that are used in a large portion of successful attacks against individuals and organizations. This type of activity can take advantage of "the teachable moment." If an employee clicks on the fake link or opens the attachment, the employee is taken to a landing page for immediate feedback and additional information. Feedback that is immediate is proven to be much more effective than feedback that is delayed.

Incentives

Employees like incentives. Consider adding them to your awareness and training program. For example, if an end user avoids clicking on a phishing email link, or answers all questions right on an information security quiz, a positive reinforcement may be to provide that employee with a reserved parking spot for a period of time, granting a few extra hours off, or praise that employee in a newsletter.

Pratum

www.pratum.com | *sales@pratum.com*