Cybersecurity Training Workshop

You are only as secure as your weakest point.
Training your staff will strengthen your defenses.

The Looming Threat of Ransomware

Malicious software used to control computer systems until the demanded ransom is paid, ransomware poses serious, pervasive risk to both individual users and large organizations. It is, however, avoidable. Ransomware most commonly enters a system through email; for instance, 31% of ransomware invasions were traced to email links and 28% to email attachments. Users can therefore evade infection through sound cybersecurity practices.

Quest's Cybersecurity Training Workshop covers:

Basic Policies and Procedures

To avoid the cunning and increasingly sophisticated tactics of today's cyber attackers, users must be aware of common security pitfalls and the risk associated with lax habits or inefficient measures. Quest's Workshop offers practical security training and helps staff understand how to recognize and evade security threats. During the Workshop, a Quest cybersecurity expert will discuss:

- The need for strong, variable passwords
- Methods for detecting phishing and social engineering attacks
- Risks of web usage
- The complexities of mobile device management
- The importance of monitoring networks and systems for security incidents

Operational and Managerial Controls

In addition to fundamental, safeguarding guidelines, an effective risk management and cybersecurity program requires executive support and operational and managerial controls. Incident response planning, configuration management, data classification, and other high-level policies bolster a company's cybersecurity.

REQUEST YOUR WORKSHOP HERE

Email programs@questsys.com

WORKSHOP DETAILS

Date/Time

What works for you and your team? Depending on your availability and requirements, we can meet with you as soon as possible, or in the near future.

Location

The Cybersecurity Training Workshop can be conducted onsite at your location or at Quest's Roseville, CA office.

Recommended Attendee Titles

If you are not the business owner and/or key decision maker, please ensure they are present; business operations/decisions are directly tied to technology requirements for most organizations. We also recommend having these key team members present:

All employees accessing the organization's virtual environment

Preferred Documentation to Review

We recommend having the following items ready to review for this Workshop, if they are available:

Current DR, BCP, and/or Cybersecurity Policies

Inventory of current tools/services/controls

Timeline at a Glance

Pre-Workshop: Schedule kickoff call, establish priorities

Kickoff Call: Introductions, agenda, expectations

Workshop: Conduct a one-day, on-site Workshop

Final Review: Quest provides Executive Summary including recommendations and action items

How can we help?®

www.questsys.com | 800.326.4220