Cybersecurity Workshop

Review your security concerns, assess your current security posture, and receive smart recommendations tailored to your organization.

Quest's Cybersecurity Workshop will:

Assess Your Current Security Posture

Bad actors, viruses, ransomware, disgruntled employees, social engineers, phishing attempts, and more — our Cybersecurity Workshop will gauge your level of vulnerability to these types of threats and others. We will review your existing security measures and/or compliance requirements to determine your unique risk factors; since business risk extends beyond the IT department, your biggest threat could be from porous work processes, or even employees that are untrained in basic security measures like avoiding phishing emails.

Identify Unknown Vulnerabilities

Along with document and policy review, we offer an optional Vulnerability Scan and/or Firewall Consultation that will discover unknown vulnerabilities like poor or nonexistent monitoring, weak firewall rules, system misconfigurations, etc.

Recommend Corrective Actions

Tailored to your organization, our recommendations will address and prioritize your security concerns, requirements, and goals. Recommendations may include, but are not limited to:

- Tech configurations
- Security policy
- Compliance requirements
- Resource optimization

Prepare Your Organization For The Future

The path to better security starts with an assessment of your existing security landscape. Quest's no-obligation Cybersecurity Workshop will provide you an Executive Summary complete with documentation and actionable recommendations — so you can take the first step toward a more confident and secure business future.

REQUEST YOUR WORKSHOP HERE

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 Workshop can be conducted online, 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:

ISO/CISO	CFO
CEO	COO

Preferred Documentation to Review

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

Security Policy   Compliance Audit Results

Incident Response Procedure

Timeline at a Glance

Pre-Workshop: Scheduling kickoff call, establishing 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?®
800-326-4220 | www.questsys.com