

Security Awareness Training

Properly training employees is one of the most important steps you can take to improve the security posture of your business. The simple fact is that no matter how good your technology may be, it is only as strong as the weakest link in the chain. Without adequate training, your employees become your weakest points. Many employees do not understand information security; or worse, have misconceptions about it. This can lead to an increase in both the likelihood of accidental data leaks and in susceptibility to targeted malicious attacks.

To address this, Alliance Technologies provides several options for employee training. The ultimate goal is to teach employees to follow good habits and, through them, maintain a healthy suspicion of potentially dangerous situations and work to minimize data leakage. Ways to achieve this goal vary from generic Internet-based training to in-depth personal consultant-based training focused on specific business concerns. To maximize knowledge retention and change employee behavior, more than one training session is likely necessary.

Internet-based training sessions are typically taken using a standard web browser, and are followed by a short quiz. Managers may access a portal and verify which employees are taking the on-demand courses and how well they do. This serves both as reinforcement of specific training topics and as a way for management to communicate the importance of security to employees.

More personal training tends to fit best with the deployment of specific projects. This helps educate employees as to how to adapt to changes, rather than resist them or attempt to work around them. A typical consulting-based training engagement starts with a short visit with corporate executive, security or IT management, and then takes a few hours to draft a custom training session. Typical training sessions last approximately one hour.

Training Benefits

- Educated employees know the risks you define as acceptable instead of determining risk on their own.
- Communicated expectations can help define a base level of competence across the entire organization.
- Trained employees follow security policies more closely than untrained employees.
- When preferred procedures are communicated, fewer people deviate from the standards.
- Regulatory compliance can be tracked through a training and testing process.

Sample Topics Covered

- Passwords and the risks that an organization faces from poor ones.
- The dangers of malware and how to protect against them.
- How attackers leverage web-based attacks and how to use the Internet more safely.
- The PCI standard and the requirements it demands of employees.
- Compliance with regulations: HIPAA/HITECH, FTC Red Flag Rules, SOX, GLBA.