Social Engineering

DATA SHEET

Testing the Human Factor

Social engineering involves testing your employees' security awareness when confronted with an unauthorized third party attempting to manipulate the employee into disclosing confidential information. This provides insight into how effective the organization's policies and procedures are at mitigating social engineering threats, how well employees adhere to them, and the level of security awareness that exists among employees.

The Compliance Overview

Information security compliance regulations and guidelines (FDIC, FFIEC, GLBA, HIPAA, HITECH, NCUA, OCC, PCI DSS) require an organization to create an information security program designed to protect confidential information, including Non-Public Personal Information (NPPI). Failure of employees to follow the security policies and procedures of the organization is a major vulnerability to an information security program.

The TraceSecurity Social Engineering Overview

TraceSecurity is a recognized authority in social engineering. Our expert information security analysts have conducted hundreds of social engineering engagements for companies across a wide range of industries. We evaluate the human factor, identify security issues that need improvement, and document compliance shortfalls. We also provide a cloud-based solution to address all the necessary functions associated with security training and policy management.

We have designed both onsite and remote test methods. When onsite, our experts use various techniques, such as "dumpster diving" and "trusted authority" disguises, to gain physical access to obtain records, files, and/or equipment that may contain confidential information. When performed remotely, our experts employ tactics, such as pretext calling, phishing, and email hoaxes, that attempt to get employees to divulge usernames, passwords, customer NPPI, or other confidential information.

Onsite Test Services Include:

- Pre-engagement setup with client (includes project planning, scope, defining rules of engagement, information gathering)
- Spoof emailing (if applicable)
- Onsite testing for:
  - Employee security and privacy policy awareness and adherence
  - Proper disposal of sensitive data
  - Access privileges
  - Sensitive area security
  - Device/system compromise
  - Technical preventive and detective controls
  - Violation reporting
- Present preliminary findings to client core team through exit interview

Social Engineering

DATA SHEET

Remote Test Services Include:

- Pre-engagement setup with client (includes project planning, scope, defining rules of engagement, information gathering)
- Remote social engineering (dependent on scope)
- Computer-based testing through email spoofing and phishing simulation
- Phone-based, pretext call testing (dependent on scope)

Extensive Reporting (for both onsite and remote engagements):

- Project overview
- Social engineering test methodology
- Executive summary
- Business and technical risks and recommendations
- Details and exposure of vulnerabilities
- Recommendations and counter measures
- Appendix samples

Options (for both onsite and remote engagements):

- On-demand generation of reports for audit, board and technical staff
- Training material provided in an extensive recorded 'Flash' module
- Automated learning management system and training management (includes access to security awareness training content)

Your Single Source for a Full Range of IT GRC Information Security Services

The complex and constantly evolving nature of IT GRC (governance, risk, and compliance) requires a range of experience and expertise that is nearly impossible for most companies to maintain internally. TraceSecurity's comprehensive suite of information security services is the answer. Our seasoned experts help enhance your security posture, reduce risk, facilitate compliane, and improve operational efficiency. To provide maximum effectiveness, the TraceSecurity information security services listed can be delivered in combination with TraceCSO, our integrated cloud-based IT GRC management platform.

- Security Assessment
- Risk Assessment
- Executive Summary
- Penetration Testing
- Social Engineering
- Web Application Testing
- Wireless Assessment
- Security Training