



Your security is our business.

Do your employees realize the potential danger of simply holding a door for someone?

Do they understand the importance of keeping their desks clear of confidential documents and their workstations locked when they walk away from them?

Do they consistently shred sensitive documents instead of placing them in the trash?

About Allied InfoSecurity, Inc.

An independent company focused only on security and staffed by certified security professionals, Allied InfoSecurity is a consulting and outsourcing provider that helps businesses improve and manage their information security programs, mitigate risk, and respond to regulatory and marketplace demands more quickly and effectively than they could on their own.

Social Engineering Assessments: Evaluating employee awareness and training

Social engineering is a collection of techniques for manipulating people into providing inappropriate access to physical and/or information assets. It's a non-technical form of intrusion that depends on human interaction. It typically involves tricking people into compromising normal security procedures by exploiting humans' desire to be friendly and helpful and to avoid confrontation.

Thus, even if your organization has implemented an optimal physical and technical information security infrastructure, your employees can compromise the confidentiality, integrity, and availability of your data. Indeed, employees are often the weakest link in a security management program and can inadvertently cause security breaches.

To ensure that your organization has a robust and effective approach to information security, you simply must know how well your employees understand your policies and procedures—and adhere to them in real-life scenarios.

Allied InfoSecurity's Social Engineering Assessments deliver an objective evaluation of your employees' awareness, training, and education. Although we customize every engagement based on each client's unique concerns and infrastructure, Social Engineering Assessments often include both external and internal reviews.

Through a Social Engineering Assessment from Allied InfoSecurity, you can:

- Understand the effectiveness of your security policies and procedures
- Evaluate the effectiveness of your employee security awareness training initiatives
- Determine whether or not physical access can be gained to your internal computer networks and/or databases
- Assess whether or not sensitive company, employee, or client information can be obtained

As part of each assessment, Allied InfoSecurity delivers a detailed report outlining your strengths and weaknesses. We often uncover socially-oriented vulnerabilities, and then document them through text and images that show our facility penetration, papers harvested from trash receptacles, and important data pieced together through online sources. Perhaps most importantly, every Allied InfoSecurity report contains actionable recommendations for resolving each issue.

As with all of our services, Allied InfoSecurity offers a uniquely flexible delivery platform for Social Engineering Assessments. This platform allows

EXAMPLES: External Assessment Techniques

Exercises	Sample Tactics
Dumpster Diving	We comb through your publicly accessible trash receptacles and harvest useful company, employee, and/or client information.
Information Reconnaissance and Data Leakage Assessment	We search publicly available online records for exploitable company, employee, and/or client information.
E-mail Phishing	We send an unsolicited e-mail message to employees asking them to submit company, personal, and/or client data via a phishing website.
Telephone Phishing	Posing as in-house helpdesk personnel, we call employees and request their system credentials.

EXAMPLES: Internal Assessment Techniques

Exercises	Sample Tactics
Facility Penetration	Using a variety of techniques (such as “piggybacking”), we enter your facility and penetrate as deeply as employees will allow.
USB Device Test	We plant USB devices and then monitor how employees handle these potentially harmful devices.
Clean Desk Policy	We visit employees’ workspaces to see if they are leaving confidential documents or other resources on their desks.
Visitor Check-In Procedures	We test the consistency and effectiveness of your visitor registration procedures.
Employee Challenge & Response	We present employees with scenarios that should raise their suspicions—and then watch to see if they ignore or address the risk.

you to contract for our capabilities as a project or through a flexible retainer—giving you the ability to choose the right approach for your business.

Our service delivery options include:

- **Allied TouchPoint™ Services.**

Our suite of a la carte services includes a full range of traditional, project-based information security services—including Social Engineering Assessments.

- **Allied Partnership Services.**

In addition to our a la carte services, we also offer this framework of longer-term contractual agreements.

Ranging from basic incident response services to highly flexible retainer services to partial or full-scale outsourcing, Allied Partnership Services allow for a truly customized relationship that reflects your current and future needs.

Offering extensive experience with social engineering assessments—and an eminently flexible approach to service delivery—Allied InfoSecurity is your best choice for addressing employee awareness, training, and education. To learn more about how we can help your organization, please visit our website at www.alliedinfosecurity.com or call us at 866-240-0094.

© 2010 Allied InfoSecurity, Inc.

The above material is presented as general information only and does not constitute legal advice or a legal opinion. You should seek the advice of legal counsel with respect to your particular circumstances.

1009 West 9th Avenue, King of Prussia, PA 19406 • Tel: 866.240.0094
email: ask@alliedinfosecurity.com • web: www.alliedinfosecurity.com

**Allied
InfoSecurity**
Your security is our business.