by Stephen Lineberry

Businesses spend a significant portion of their annual information technology budgets on high-tech computer security. But the firewalls, vaults, bunkers, locks and biometrics those dollars buy can be pierced by attackers targeting untrained, uninformed or unmonitored users.

Few companies properly address the human element of information security. “There are times when the human element is the leaky faucet” that spills sensitive information, says Debra Murphy, a consultant who is vice president of marketing for Rapid7, a Boston-based security software company that performs vulnerability assessment, network penetration and social engineering testing. One cause for the information trickle linked to employees is the pressure many are under to constantly improve customer service. “People are being measured on helping customers and providing a great customer experience,” Murphy says. Social engineering scam artists, who use deceptive and manipulative tactics on individuals to gain unauthorized access to information, pounce on that customer-focused mandate.

Some of the best tools for fighting social engineering attacks are security awareness training and social engineering testing. The effectiveness of these controls will vary based on the quality of their implementation, including follow-up and retraining.

Social engineering testing, by its very nature, can be difficult to conduct without third-party assistance. One option is to engage an information security organization to conduct testing. The testing can uncover areas in which an organization is most vulnerable so that risk can be assessed and mitigation strategies can be formulated and implemented.

While prices vary, hiring an outside firm to conduct social engineering testing typically costs between $10,000 and $15,000. Rolling social engineering testing into a larger security penetration engagement can reduce the cost of the social engineering component, says Jim Patterson, director of consulting for Rapid7.

A meaningful social engineering audit
**Costly Incidents**

In the 2006 CSI/FBI Computer Crime and Security Survey conducted by the Computer Security Institute and the FBI, 313 computer security professionals reported a total of $52.49 million in losses linked to computer security incidents for 2006. The following is a sample of the kinds of attacks reported and the related financial losses:

- **Virus contamination:** $15.69 million
- **Unauthorized access to information:** $10.62 million
- **Laptop or mobile hardware theft:** $6.64 million
- **Theft of proprietary information:** $6.03 million
- **Insider abuse of Internet access or e-mail:** $1.85 million
- **Bots (zombies) within the organization:** $923,700
- **System penetration by outsider:** $758,000
- **Phishing in which your organization was fraudulently represented as the sender:** $647,510
- **Password sniffing:** $161,210

must involve people who are knowledgeable about social engineering techniques and are creative enough to mimic the methods of real attackers. Rapid7 typically tests in a double-blind engagement, coordinating primarily with internal audit groups in large companies or the head of IT in smaller businesses. The testers set out knowing little about the client company, Patterson says. The IT staff and other employees of the target firm are not alerted to the possible attack.

**ATTACK SIMULATION**

The following example is based on an actual social engineering test. For privacy, some information has been altered or omitted; however, the techniques and results are accurately portrayed.

A common way to prevent unauthorized access to secure information is to require proof of identification. The goal of this test was to manipulate a bank employee into processing a transaction without obtaining any form of identification from the customer, who in this case was a social engineering tester.

Through simple observation of the target, the tester gathered information critical to his attack. A photo ID was generally required when a person requested a transaction. Friday afternoon was a particularly busy time for bank employees, with a typical wait time in line of 22 to 25 minutes.

Closing time was 5 p.m., and the entrance door typically would be locked a few minutes prior to closing. Employees could easily overhear customers' conversations because of the size of the space.

The attack was scheduled to begin on a Friday at 4:30 p.m., when distraction was highly likely due to heavy activity and the approaching weekend. The social engineering tester arrived at 4:30 p.m. and took his place at the end of the line. The tester engaged others waiting in line in friendly conversation. The tester joked about the trials of his day, which included getting a speeding ticket that caused him to be behind schedule. An employee locked the entrance door a few minutes before closing. The tester then continued to make conversation as he waited in line. His turn came a couple of minutes before closing.

The tester complimented the employee for the patience the employee had shown with a rude patron.

Prior to being asked, the tester removed his wallet and searched for his driver's license, which, of course, he could not find. The tester continued, somewhat frantically, to remove contents from the wallet in search of his license.

At this point, the employee played right into the tester's hands. The employee referred to the traffic ticket the tester had discussed while in line, and the tester appeared suddenly enlightened. He told the employee that he had likely stuffed his license in his glove box along with the traffic ticket. He apologized and asked the employee to please wait while he went to his car to retrieve his license.

The employee, knowing that the entrance door was locked and that it was closing time on a Friday, told the tester not to worry about it. The employee processed the transaction, gave the tester the information he sought and told him to enjoy his weekend.

**EXECUTIVE SUMMARY**

- **Social engineering attacks involve the use of deceptive or manipulative tactics** on an individual to gain a result—often to gain unauthorized access to information assets. The practice sometimes is referred to as soft hacking and often is used to gather intelligence for a subsequent hacking attack.
- **Technically savvy CPAs have the skills to analyze** a company's information security climate, search for patterns in security-related data, make recommendations to management and formulate security policies and procedures.
- **Testing by a third-party contractor** can pinpoint whether an organization is vulnerable to social-engineering attacks. Such testing can shed light on whether employees adhere to the information security guidelines set out in policies and procedures.

**Stephen Lineberry,** CIA, NSA IAM/IEA, is information systems audit manager for KraftCPAs PLLC. His e-mail address is slineberry@kraftcpas.com.
The social engineering tester successfully induced:

- **Familiarity.** The employee had likely heard enough of the tester’s conversation with others and no longer viewed the tester as a complete stranger.
- **Sympathy.** To the employee, the tester appeared to have had a trying day, but seemed to be taking it all in stride. He had even admitted that he deserved the speeding ticket and he couldn’t fault the police officer for doing his job.
- **Comfort and Trust.** The reason the tester did not have his license seemed perfectly plausible to the employee.

"At the end of the day, it’s about getting someone to violate a policy," says Patterson of Rapid7.

Social engineering attacks are often used to gather intelligence that might be useful in a subsequent hacking attack. During a recent engagement, Rapid7 was hired to conduct penetration testing for a business that offers online sales of gift cards. The tester’s goal, Patterson says, was to get someone from within the company to open an e-mail message containing a Trojan horse that would install malicious software giving the attacker control over the victim’s computer and, thereby, access to customer credit card information.

The tester entered bogus credit card information with his order, which triggered a phone call from an employee whose job it was to manually enter all payment information from the seller’s online orders. The tester offered to send the correct information to the business in an e-mail with an attached document. The phone conversation was designed to lower the guard of the employee, who might not have opened the e-mail had it come from a complete stranger. In the end, the employee opened the e-mail and attachment, Patterson says, and welcomed in the Trojan, allowing the tester to break through the firewall and gain access to 25,000 credit card accounts.

Fred Cantz, senior manager, forensic accounting and litigation support, for Smart Business Advisory and Consulting’s Philadelphia office, cautions that such social engineering audits can open up a host of employee relations issues and sensitivities. He suggests that the results of testing should be used to aid in training rather than to discipline employees.

**THE TRAINING GAP**

Many information security managers and administrators may feel uncomfortable as trainers. While knowledgeable about technology, often they’re not as good at dealing with policies and procedures and the training aspects of technology," says Danny Jeter, senior manager and consultant with Jackson Thornton Technologies.
a business spun out of the Montgomery, Ala.-based accounting firm Jackson Thornton.

That disconnect, combined with discomfort relating to personal privacy issues, is among the chief reasons that a large percentage of organizations do a poor job managing the human element of information security.

Many critical controls that support information security are non-technical. Observing non-technical controls may reveal much about the strength of an organization's information security. A technically competent CPA—especially a CPA who is a Certified Information Technology Professional (CITP), Certified Fraud Examiner (CFE) or a Certified Information Systems Auditor (CISA)—can add value to a company by observing and analyzing issues that affect information security and then communicating concerns and recommendations to management.

CPAs understand internal controls and can assist companies in adapting control concepts to protect the confidentiality, availability and integrity of valuable assets. Cantz says CPAs can perform trend analysis and search for patterns in security data. They can be assets in drafting policies and procedures for safeguarding financial and customer data and also play a role in training employees to abide by the rules.

"CPAs and IT have to work as a team," says Cantz, a CPA, CFE and former supervisory agent with the U.S. Postal Inspection Service. "I don't think CPAs can do it better or cheaper or faster. But working hand-in-hand with IT, they can design a program that will assist in combating the social engineering challenges of today's workplace."

Patti Perdue, a principal with Jackson Thornton and the partner-in-charge for Jackson Thornton Technologies, suggests that all partners and managers in her firm ask their clients questions including: How do clients protect confidential information stored on the network or business computers? How often do they check for employee compliance with the requirements? Are employee passwords changed at least annually? Does an independent third party evaluate controls periodically?

To foster a culture that is information security aware, company management, assisted by qualified CPAs, should begin by asking the following questions:

■ Are employees educated and aware of common information security threats?
■ Do they write down or freely share passwords with others?
■ Do visitors freely move about facilities without facing barriers to entry, such as a requirement to wear a company-issued badge?

■ Is it common to see sensitive information, such as completed employment applications or client documents containing Social Security numbers, accessible in unmonitored or otherwise unsecured areas?

■ What is the prevailing employee attitude regarding information security controls? Are enforced information controls viewed primarily as a nuisance or a necessity?

No system is immune to human ingenuity. Effective information security must be culturally ingrained and backed by strategies and processes that are continually tested, taught, measured and refined.
Copyright of Journal of Accountancy is the property of American Institute of Certified Public Accountants and its content may not be copied or emailed to multiple sites or posted to a listserv without the copyright holder's express written permission. However, users may print, download, or email articles for individual use.