

The Perils of Human Nature

By Michael McKinley, *Chief Financial and Operating Officer, Allied InfoSecurity*

People have a profound impact on any information security program. From the desire to be helpful to an aversion to conflict, certain human tendencies create or exacerbate security vulnerabilities. As Allied InfoSecurity's Michael McKinley explains, human beings can be exploited through "social engineering"—a collection of techniques used to manipulate people into performing actions or divulging confidential information. In this article, McKinley outlines five socially driven vulnerabilities, provides real-world examples of how they can be exploited through social engineering, and offers practical advice for addressing this often overlooked aspect of security.



Your security is our business.

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

© 2010 Allied InfoSecurity, Inc.

The following 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.

About the Author: Michael L. McKinley



Michael McKinley is a co-founder of Allied InfoSecurity, Inc., serving the business as chief financial and operating officer. To this role, Mr. McKinley brings a wide-ranging and distinguished background in corporate financial management and information security operations and policy development.

Prior to co-founding Allied InfoSecurity, Mr. McKinley served as financial controller for the \$400 million Campbell Soup Food Service Division. In this position, he led financial planning, projection, and control functions for the divisional supply chain and managed nationwide relationships with food plant controllers and co-manufacturers. In addition, he has managed the divisional compliance program for the Sarbanes-Oxley Act and all other corporate compliance requirements.

Mr. McKinley has also held numerous financial positions within Campbell Soup, including divisional finance manager and senior manager of financial planning and analysis for the Campbell Away From Home Division, as well as financial manager in the company's North American Soup Division.

A distinguished graduate of the United States Air Force Academy, Mr. McKinley started his career as a military intelligence officer. He served in numerous overseas and domestic assignments of increasing responsibility—culminating in a two-year Pentagon assignment as chief, Defensive Information (Computer) Warfare Doctrine and Strategy. While at the Pentagon, he developed, implemented, and managed force-wide policy, doctrine, and organizational constructs guiding the \$250 million Air Force program for the protection of mission-critical information and information systems from computer-oriented threats.

Before the Pentagon, Mr. McKinley served five years in headquarters and field postings in Europe, including chief, Intelligence Plans; command speech writer and briefer; and duty director, Intelligence. He also led intelligence teams in Saudi Arabia and Italy supporting United Nations operations in Iraq and Bosnia.

Think fast: What are the top five threats to the confidentiality, integrity, and availability of your organization's information? If you rattled off technical vulnerabilities, you're only partially right. That's because for virtually every organization, one of the biggest threats to security isn't technical. It's human, or more specifically, human nature and the resulting behaviors of your employees.

Although there's no question that every human being is unique, for the purposes of this article, we're going to make some generalizations about people. We don't intend these broad-brush statements to be offensive in any way. Rather, we want to illuminate some important points about potential vulnerabilities your employees may be creating or enabling on a daily basis.

Understanding the basics

Before delving into the perils of human nature, let's take a step back to clearly explain why there's such potential for issues. The reason is something known as "social engineering."

Social engineering is a collection of techniques used to manipulate people into performing actions or divulging confidential information. This term usually applies to trickery for information gathering or access to computer systems. In many cases, "social engineers" never come face to face with their victims—who are merely pawns in their scheme to circumvent security measures.

If you've ever seen a movie or read a book featuring a private investigator, you may be familiar with some of the techniques of social engineering—for example,

posing as someone else, currying favor with a phone operator or other service employee, or rooting through trash to find valuable information.

“**Social engineering is a collection of techniques used to manipulate people into performing actions or divulging confidential information.**”

Imagine those and other tactics being used to compromise the security of your business. Now, ask yourself: Am I certain that my employees are aware of social engineering techniques? Would they respond in a manner that protects the security interests of the company? Or would they inadvertently provide access to confidential information?

The human impact on information security

Allied InfoSecurity's practitioners have performed numerous social engineering assessments, giving our clients unprecedented insight into the "weak link" that human behavior often creates. In conducting those assessments for companies of varying sizes and industries, we've observed some common threads of human nature that lead to potentially serious information security vulnerabilities.

Vulnerability #1: Most people want to be helpful.

Your parents probably raised you to be courteous and thoughtful. So when someone's behind you in an entranceway, your natural inclination may be to hold the door. Similarly, when someone asks for your assistance—whether in person, over the phone, or via email—your first reaction may be to say, "Sure, I'd be happy to help you out." Unfortunately, "blind" courtesy can have dire ramifications in the realm of information security.

At Allied InfoSecurity, we test employee awareness and education about physical security by attempting to “piggyback” or “tailgate” through card-protected doors. Almost invariably, it works; someone politely holds the door and allows us access to the facility. Another variation on this theme is card-controlled elevators. More often than not, a friendly individual will insert his card and then offer to help: “What floor do you need?”

Most people’s strong desire to be helpful also comes into play with our e-mail and telephone phishing exercises. In these tests, we contact employees via phone and/or e-mail and then ask them to provide information that would enable us to penetrate the organization’s infrastructure.

In some cases, we pose as headhunters and lure employees to a bogus website, where we request sensitive information. Other times, we pretend to be helpdesk personnel who are planning for a “weekend migration.”

“If you don’t provide your log-in credentials to me today,” one of our practitioners may say, “you’ll probably have to wait a few hours to get to your files on Monday. It would really help us out, and you, too, if we could take care of this today.”

As a corporate IT or business manager, you’d probably be stunned to know how often employees offer up the data. It’s even scarier when you consider that technical penetration testing and network vulnerability assessments don’t capture these risks.

Vulnerability #2: Most people strive to avoid confrontation.

With some rare exceptions, most people simply don’t like to initiate confrontations. That’s particularly true when it comes to information and physical security. Because of this aspect of human nature, it is easy to pull

“ In conducting social engineering assessments for companies of varying sizes and industries, we’ve observed some common threads of human nature that lead to potentially serious information security vulnerabilities. ”



off a ruse and gain access to a corporate facility. For social engineering assessments, Allied InfoSecurity practitioners have posed as “building inspectors” or representatives from a company’s “home office.” (And that’s only when employees don’t just hold the door for us.)

People simply don’t want to question another person—and be wrong. So instead of taking that chance, they turn a blind eye to mysterious strangers, thereby empowering them to gain physical access to the building and other company resources.

During one social engineering assessment, a security guard seemed suspicious of my colleague and me. Having successfully entered the facility, we were having coffee in the company break room when this young man cautiously approached us. When we realized he was likely to question us, we staged an argument between the two of us. The diversion worked; the guard headed back to his desk and left us—unauthorized visitors—unattended inside the building.

Vulnerability #3: Most people want convenience (and many whine when they don't get it).

Even simple security policies and procedures can create “headaches” and “inconvenience” for employees. Having to continually sign back in to a locked computer, being required to conceal sensitive documents throughout and at the end of the day, and being asked to walk through only guarded entrances are only a few examples of policies that may cause employees to complain.

But maintaining—and, more important, enforcing—these types of policies are absolutely critical to the security of your business.



We've seen numerous facilities with four entrances, only one of which is guarded. It raises the logical question: Why have so many entrances if they aren't all secured? The answers often come down to employee preferences.

People want to use the door that's closest to the parking lot, saving themselves extra walking to and from the building every day. Similarly, employees who smoke often want to get in and out of the building quickly for cigarette breaks. In both cases, employees are creating major opportunities for piggybacking/tailgating, and denying security guards the chance to perform proper check-in procedures.

Vulnerability #4: People can be messy.

When it comes to information security, maintaining a tidy workspace is about more than mere aesthetics. Companies should maintain “clean desk” policies to ensure that sensitive information is never left unattended in an employee office. Instead, it should always be tucked away in a drawer, perhaps even under lock and key. The same caution should be applied to files sent to network printers or duplicated on copiers. And, of

“ People simply don't want to question another person—and be wrong. So they turn a blind eye to mysterious strangers, giving them physical access to the building and other company resources. ”

course, when it's time to dispose of sensitive documents, they should be shredded.

While performing social engineering assessments, we've found sensitive documents on desktops, in printer trays, and on copiers. Some of those documents—such as employee directories—have empowered us to further penetrate the organization with other social engineering techniques.

We've seen instances where documents are left in plain view at the end of the day—giving access to cleaning staff and, in other cases, leaving files literally visible from outside the building thanks to large first-floor windows.

Vulnerability #5: People are curious.

USB devices, or “thumb drives,” have become commonplace in today's offices. Employees increasingly rely on them for easy file storage and transfer. But these portable hard drives can house viruses and other forms of malware—and people's “need to know” can invite the trouble into your IT environment.

As part of many social engineering assessments, Allied InfoSecurity plants USB devices in or outside a company's facilities. Even though many employees have been trained not to insert unfamiliar devices into company computers, often their curiosity gets the best of them. And that can create huge problems, as these drives may contain viruses or other malicious software. In fact, in our tests, we frequently gain full control of PCs when users plug in our USB devices.

Strengthening every link

None of us is likely to change these and other fundamental characteristics of human nature. Yet companies are ill-advised to ignore the impact of human behavior on their information security. Fortunately, there are strategies and tactics you can take to help educate employees and mitigate the risks.



For starters, a social engineering assessment can help to test your employees' awareness of and compliance with your company's security policies and other best practices. Depending on the results of that analysis, you can begin to explore some specific actions that can help strengthen the human link.

An enterprise-wide employee awareness and training program is almost always a good idea. In addition to a formal program, it's important to foster an informal culture—from the top down—that encourages employees to question unfamiliar individuals in the building or on the phone. In this culture, there's no retribution for an employee who challenges someone who turns out to be legitimate.

There are also some very concrete tactics that companies can take, such as installing “mantrap” doors that allow only one card-carrying person to enter a building at a time or increasing the availability of shredding equipment for proper disposal of sensitive documents.

Above all, be certain that you've thought through and addressed the breaches your employees may be creating for your company. If you aren't sure what those breaches may be—or how best to address them—enlist the help of security practitioners with experience and expertise in social engineering testing.

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.

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