Chapter 1

Social Engineering: Risks, Threats, Vulnerabilities, and Countermeasures
by Jack Wiles

Jack Wiles is a security professional with over 30 years of experience in security-related fields, including computer security, disaster recovery, and physical security. He is a professional speaker and has trained federal agents, corporate attorneys, and internal auditors on many computer crime-related topics. He is a pioneer in presenting on subjects that are now being labeled “Homeland Security” topics. Jack is a co-founder and President of TheTrainingCo., which runs the well-known Techno Security and Techno Forensics trade shows. He is in frequent contact with members of many state and local law enforcement agencies as well as special agents with the U.S. Secret Service, FBI, U.S. Customs, the Department of Justice, and the Department of Defense. He was appointed the first President of the North Carolina InfraGard chapter, which is now one of the largest chapters in the country. He is also a founding member and “official” MC of the U.S. Secret Service South Carolina Electronic Crimes Task Force. Jack is also a Vietnam veteran who served with the 101st Airborne Division in Vietnam in 1967–68.
Chapter 1 • Social Engineering: Risks, Threats, Vulnerabilities, and Countermeasures

Introduction

Some of the things I will discuss in this chapter have been on my mind since the mid-1980s. I believe it’s time I put them in writing and present my thoughts on what I believe could be the most effective and dangerous threat to any security plan: social engineering! This age-old threat has taken on a new meaning as what I collectively call “bad guys” have continued to use the art of the con to gain access to intellectual property and, if necessary, the buildings that house it.

This chapter isn’t meant to be read as a complete story from beginning to end. Social engineering and ways to prevent it are subjects with many meanings. This will be more of a potpourri of tips, tricks, vulnerabilities, and lessons learned from 30-plus years of dealing with these issues. As an inside penetration team leader, I used every exploit I could to conduct a successful inside penetration test. It was during those years that I gained most of my social engineering experience. These skills helped me eventually hang up my dumpster-diving penetration team clothes and retire from the tiger team world UNDETECTED! Although I came close several times, I was never stopped or reported to security as a possible burglar or corporate espionage agent, even though that’s what I effectively was while I had our teams inside their buildings.

If you think this chapter has a strong risk management flavor, it was intentional. Just about every area of concern with security today is a risk management issue. This chapter, and most of the others in this book, are chock full of what I like to call Techno Tidbits of useful risk management countermeasures. Hopefully, many of them will be topics you might not have considered in the past as you put together your security plan. External, internal, and information system auditors should pick up a few ideas for things that should be added to their audit process.

How Easy Is It?

Way back in 1988, I was part of an internal security team for a large corporation. On several occasions, I had the opportunity to hear some of the conversations that went on when a cracker (bad guy hacker) group targeted a victim by calling them on the phone. They were using social engineering skills to gain access to proprietary information, including passwords. I’ll never forget what I heard one experienced cracker say to a cracker-in-training: “Social engineering is the easiest way to break into a system.” He then followed up that comment by saying “The stupidity of the average system administrator amazes me.”

That was almost 20 years ago and it was the first time I had heard the words social engineering. Why do I think of it as a tool that could be used by any “bad
guy” from a cracker to a terrorist? Social engineering is what I believe could be the most effective and dangerous outsider–insider threat to any security plan.

Over the past 15 years, I have learned firsthand just how easy it is to be an effective con man as I lead several inside penetration teams into clients’ buildings who hired us to test their vulnerabilities. Not one time did we fail or get caught as we roamed their buildings pretending to be employees. Everyone we encountered while doing our thing thought we belonged there.

Human Nature: Human Weakness

This is certainly not the first time anyone has written about the effects of social engineering. It doesn’t take much searching on the Internet to find material on the subject, and in almost every article you will note a common thread. In each case, the social engineer turns our normal human nature of wanting to be kind, helpful, and sympathetic into a weakness they can exploit.

If we looked at this through the eyes of a risk manager performing a risk assessment, our untrained and unaware human nature could be considered a major vulnerability, threatening just about everything important to our company. We’ll talk about possible countermeasures to these threats throughout the rest of the chapter.

The reason I digressed into a full discussion about a risk assessment of the threat of social engineering is because I don’t think many people have performed a detailed risk analysis. Since social engineering is a truly formidable threat, you need to know how vulnerable you are (at work and home) and what you can do to reduce those risks.

Any risk assessment needs to consider at least four things: risks, threats, vulnerabilities, and countermeasures.

Risk Management:
Performing a Mini Risk Assessment

I recently had the opportunity to purchase my first boat. It’s not huge, but it is just big enough for me to use as a floating mini-office a couple of days a week when the weather is nice. Just for fun, let’s do a mini risk assessment of some of the risks, threats, vulnerabilities, and countermeasures associated with my new floating office. This isn’t intended to be extensive (I’m sure you will think of things I didn’t mention here). I just wanted to give us practice using terms most associated with risk assessments and risk management.
What Do I Have at Risk?

Being out on the water all day, my life is the first thing that comes to mind as a risk. The boat itself is also at risk, though I have passed some of the financial risk along to an insurance company, which is what we do with a lot of risks where it makes sense. Any equipment on the boat is at risk of not only sinking but of possibly being dropped overboard, or being soaked by a large wave. A sudden thunderstorm could cause problems. Depending on lake conditions, too many other boats could cause a problem. The battery in the boat could die causing me to lose all power and even strand me on the lake. As you can see, when you consider what you have at risk, you will immediately start to consider some of the threats that could possibly increase your risks. What I have at risk on the boat is everything I could lose if something bad happened. Let’s call all the bad things that could happen “possible threats.”

What Are Some Possible Threats?

We’ve already mentioned a few possible threats, which are different than those surrounding my home office. Weather could certainly be a threat, as could simply hitting something as I was moving from one place to another on the lake. The threat of a sudden thunderstorm, or of being hit by another boat, always exists. There isn’t much risk of being hit by a car (hopefully), or suffering from a commercial power outage while I’m aboard. The possible threat of theft should be small as long as I keep an eye on my equipment while I’m launching the boat. Overall, the threats, which could possibly hinder my ability to conduct business from my boat, would be lower than most places. (Am I looking for reasons to work from my boat or what?)

What Are Some of the Possible Vulnerabilities?

I would be much more vulnerable to severe weather changes out on the lake than in my home office. I would also be vulnerable to lake conditions in general at any given time. (This is a large lake about 20 miles long.) For a few days following a heavy rain, hundreds of semi-submerged items float down stream. I would certainly be vulnerable to someone losing control of his or her boat and crashing into mine. If I didn’t know the depth of the water I was in, I could possibly run aground or hit something in water that was shallower than I thought it was. It would most likely just be an inconvenience, but as in any vehicle, I could run out of fuel. I mentioned not being affected by commercial power failures, but I could easily run my only battery down to where I couldn’t start the engine to return to the marina. In addition,
though I am always very careful, I could possibly fall overboard—a difficult problem when you’re on the water alone.

**What about My Countermeasures?**

I really enjoy talking about countermeasures. The word even sounds cool. You have all of these things that you have identified as yours and they could be at risk out there in the boat. You have considered the possible threats and how vulnerable you might be as you encounter them. Now, what can you do to lower your risk and decrease your vulnerability?

I’ve learned a lot during the few months I have had this new floating mini-office. Some of my newfound countermeasures are

- I only try to be on the lake when most other boaters aren’t out there.
- I check the weather forecast every time before I head to the lake.
- I will install a second marine battery to insure I always have power.
- I have made sure special waterproof cases are used for my computer and cell phone.
- I carry a small inverter onboard to provide me with 110 volts AC from the boat battery.
- I make sure the marina and my family are always notified of where I will be, and when I expect to return.
- I always carry a small marina radio onboard.
- All data on my computer and cell phone have backup copies on shore.
- I wear a self-inflating life vest at all times.

I’m sure many more issues could be addressed in this mini-assessment, but the point is we all need to at least be familiar with, and understand, our risks at home and work. Included in this book is a detailed chapter titled “Personal, Workforce, and Family Preparedness,” which contains a wealth of information for lowering your risk in some of the most important areas of your life.

**Outsider–Insider Threats**

For my definition here, let’s consider the outside threats as those coming at you from the Internet or dial-up modem (You do know where all of your dial-up modems are; don’t you?), or a simple phone call from a total stranger. The reason I mention
Chapter 1 • Social Engineering: Risks, Threats, Vulnerabilities, and Countermeasures

dial-up modems is because there are still many of them out there. Many maintenance ports on older PBXs, building environmental controls, air handling systems, and access control systems still use them and probably will continue to rely on them well into the future.

I'm not considering insider (current employee) activity in this chapter. Even though malicious insiders can use social engineering in a number of ways, the countermeasures for that kind of activity can be much different. For this discussion, let’s consider outsider–insider threats as people who never were employees and didn't belong in the building.

This would be the category my inside penetration team would fit into. When we roamed through buildings unchallenged, we definitely didn’t belong there (other than being hired to try to get there). Someone checking out your building for possible espionage or future terrorist activities would also fit in this category. In theory, some employee inside the building should eventually figure out that there is a “Trojan horse” in the camp. Someone who has gotten past whatever security there is at the perimeter where entry was gained. There is a good chance they used some form of social engineering to get there.

Here's why I keep preaching about this subject and the subject of knowing who is in your building at all times. For more than three decades now, I have observed what I believe is a lack of awareness of this concern. Over the years, I have seen comparatively few articles address this silent but formidable threat. Remember, when I spent those years doing this for a living, we were hired expecting to get caught in an attack that was designed to become bolder the longer I had the team in a building. Toward the end of just about every job, we were openly walking around like we worked there, almost hoping to get caught by someone. We never did!

We were good, but I suspect there are many “bad guys” out there who are much better at it than we were, and they won't try to get caught in the end like we did. We were also working under a few self-imposed rules that the real bad guys could care less about. Using forced entry, like a crow bar to get through doors or windows, was a no-no for us. Our main tools were a cool head and our social engineering skills whenever it made sense to use them.

The Mind of a Social Engineer

I'm not sure I'll do this part of the chapter justice, but I'll try. Although I've been involved with using and teaching about social engineering for almost two decades now, I didn’t really understand why it works so well until about five years ago. When I was out in L.A. for a meeting on financial crimes security, I purchased a very interesting book titled The Art of Deception by Kevin Mitnick and William Simon.
Just above the title on the cover of the book in red letters are the words “Controlling the Human Element of Security.” I have since read most of the book, as well as many of the reviews written about it on Amazon. I found it to be well written and full of many good examples of how social engineering works and how companies can try to defend against its use. I also learned quite a few new approaches to targeting potential victims I had never thought of before. A social engineer will continuously learn increasingly clever ways to take advantage of how our minds work. The perfection of these skills comes from what Kevin Mitnick mentions in the *The Art of Deception: practice, practice, and more practice!* That’s what every good social engineer does a lot of.

**The Mind of a Victim**

Any one of us, at any time, could easily become the victim of some form of social engineering. I believe it isn’t possible to completely eliminate all risk, but some things can and should be done to reduce the risk as much as possible. I’ll address some of them throughout the rest of this chapter. Without some form of training and that same *practice, practice, and more practice* idea in learning how to prevent being a victim of social engineering, you could easily become a victim and not even know it.

Our minds work in very trusting and predictable ways, and that means exaggerated deviations from the norm might never be considered. This is what social engineers count on. Without awareness of the problem and without an understanding of how our minds can be fooled, there is little defense against social engineering. For this awareness training to be of any benefit for an organization, it must include every employee of every organization.

We see things all day long and we don’t pay close attention to certain details because they are too familiar to us. That’s exactly how the illusions that magicians call magic work. It’s also why so many magic tricks are related to simple everyday things like a deck of cards. I use magic in much of my training and it really adds a lot to the attention span of the people in front of me. They are all so used to seeing those 52 cards that they don’t think about how the different card gimmicks used in most card tricks work. Most of these illusions are self-working yet almost mind boggling to the unsuspecting mind.

Here’s a quick example of a short riddle that catches many people off-guard because of the way our minds work:

*I have two coins in my pocket that add up to 30 cents. One of them is not a nickel. What are the two coins?*

I’ll answer the riddle at the end of the chapter.
Countermeasures: How Do Bad Guys Target Us, and What Can We Do About It

As I mention some of the countermeasures I consider important, I’d like to do so in a more novel way. This list certainly doesn’t include all of the possible countermeasures for trying to prevent a successful social engineering exploit. The Internet contains many other articles written by very experienced writers on the subject. I have read several of them and I agree with just about everything they suggest for countering social engineering.

The following is a list of some of the countermeasures I have recommended to companies we have performed penetration tests for over the years. Social engineering played a very important role in every test. In each case, it was the primary tool we used to perform the physical penetration of the client’s building(s). Time after time, when we presented our after-action reports, most of the success of our penetration test was attributed to our inside team.

Most of our clients quickly reacted to attempts to gain access from the outside over the Internet. Their intrusion detection systems worked pretty well, and their incident response plans were effective. They were completely unprepared, however, for us simply walking into their buildings and acting like we belonged there. Once inside, we pretty much owned the building and everything in it. In the larger buildings, there were so many desks it didn’t seem anyone knew everyone else. That was what we liked to see. Easy pickings.

What follows are some of the most important things for you to consider as you plan your defense against possible social engineering attacks.

Key Control

The types of keys used in most buildings have remained virtually unchanged since Linus Yale invented them in 1861. Just about all of our homes, and most businesses, still use his pin tumbler locks for their primary physical defense. I have no way of knowing how often the master, grand master, and possibly great-grand-master key systems in buildings are changed. I do suspect it’s not very often. This can be an expensive process. Recently, I walked into a public restroom in a large office building and saw a full set of keys, including the building master key, hanging from the paper towel dispenser. I suspect the janitor had just filled the towel rack and left his keys hanging there. In the hands of the wrong person, that collection could prove devastating.
While using our social engineering skills during each penetration test, our team always tried to make friends with the cleaning crew. Sooner or later, we would need to ask a favor and borrow their keys for a few minutes. (Typically, their keys would open all of the doors on that floor and sometimes the entire building.) That was all it took for us to make a copy with the portable key machine we brought with us in a small bag. Very few people have any idea how keys and the locks they open work. This is another area of physical security that has changed greatly during the past few decades. I became a bonded locksmith back in the 1970s and found it fascinating. Back then, I couldn’t even purchase lock picks or key blanks until I graduated from a credited locksmithing school and had proper identification. Now, about 30 years later, we have much more at risk in general, and anyone can purchase lock picks at several local hardware stores or from Internet-based stores with no questions asked.

Regarding the use of lock picks to get into buildings and rooms, I doubt many “casual” social engineers use them. They do require a lot of that “practice, practice, and more practice” stuff needed for any social engineering skills. The availability of these devices for anyone to purchase is something corporate security specialists need to consider as they plan their countermeasures.

**Tip**

Attempt to set up some form of key control if you don’t already have a system in place. It is very important to know who has the keys to your kingdom as well as how many doors can be opened by each key. It is very seldom a good idea to have one key that opens everything in the building. It may be more convenient for certain things, but it does create the security concern of controlling who has those keys and how easily they can be duplicated.

Master keys are an additional concern if you rent space in a large building or office park. You might have a very strict policy of your own for your company, but if the management company that handles the building rentals isn’t as careful with their master keys, the entire building is at risk. Unless the keys are of a high security design like the Medeco line, they can be duplicated anywhere. Even if the disgruntled building maintenance person turns in his keys upon being fired, there is no way to be sure he didn’t have copies made. You should ask the building manager about his policy regarding the issuing and security of the master keys. It will let them know you are aware there are keys to your office that are not under your control.

Install special locks on critical doors. Highly pick resistant Medeco locks are some of the most effective. In addition to providing addi-
tional security, they add another level of due diligence should you need to document your attempts to prevent intrusions.

Conduct special employee awareness training for everyone who works on the evening and night shift. That's when I took our team into their buildings most of the time. We used our social engineering skills to befriend these people and to the best of my knowledge, we were never reported by any of them.

Another prime target during our evening and night visits was the janitorial team. The main reason we always tried to befriend the people on the janitorial team is that they usually had those important keys we were trying to get our hands on. These are some of the most important people in your company when it comes to protecting your buildings when most employees are gone. They spend some time in just about every room in the building each week. If you don’t train anyone else in your company, these people need to be well trained on how they can help. They should be made aware of your security policies and what they should do if they see anything suspicious. This would include strangers, suspicious packages, doors that are opened which should be locked, and so on. They are one of your most valuable resources. Tell them that, and teach them how they can help.

Dumpster Diving Still Works

“Dumpster diving” is one of the easiest ways to find out information about a company or its customers. This is sometimes referred to as “trashing,” and there have been a number of articles discussing what worked and what didn’t for some experienced “trashers.” One article discussed “advanced trashing” and ways to talk yourself out of a confrontation if you get caught. I’d be willing to bet that only a very small percentage of “dumpster divers” ever gets caught. As simple as this problem seems, it isn’t given much attention by most companies.

What kinds of things can you find in a company’s dumpster? You would probably be shocked if you started looking through your own dumpster occasionally. (I highly encourage you to do just that.) There may be old company directories (still quite accurate and very valuable for use in social engineering), pieces of scrap paper with phone numbers and possibly passwords written on them, last month’s customer lists that were discarded when the new list was printed this month, employee lists with home addresses and Social Security numbers, and so on.
It doesn’t take much imagination to think of all of the potential problems that could have their beginnings right there in your trashcan. Someone who is trying to pretend that they work for your company can use the old company directories. Most names in the directory, their work locations and their titles remain the same from update to update. These discarded directories are some of the most prized finds of any “dumpster divers” looking to get information about your company. The discarded scraps of paper with the passwords on them are also prized finds. Many times, they are discarded just because they were no longer sticky enough to stay on the terminal they were attached to, so a new one was written and the old one thrown in the trash. Last month’s customer list will probably wind up in the hands of your competitor if the wrong person gets his hands on it. The employee list with the home addresses and Social Security numbers on it will cause different problems if it winds up in the wrong hands.

What can you do about this problem? For one thing, we can all be a little more careful about what we throw in the trashcan. Management commitment to correct this problem, along with employee awareness of the problem will help solve it. This commitment usually involves the shredding or burning of all-important documents. If a company is going to invest in their own shredder, I always recommend a crosscut shredder over a strip cut shredder. Strip cutting is better than nothing, but crosscutting is much more secure. It turns the documents into small pieces of material instead of long strips that can be reassembled. I guess it’s theoretically possible to reassemble a strip cut document, but if it falls into a bin with a large number of other strip cut documents, it will create the world’s most difficult jigsaw puzzle.

Old habits die hard, and this one will probably be no exception. As a country, we have been throwing away just about everything since the end of World War II. During the war, security was on everybody’s mind, and each person encouraged their friends and neighbors to be careful what they said and what they threw away. (I wasn’t around during World War II, but I was the product of a happy homecoming after the war.) As individuals and companies, we need to bring back just a little bit of that way of thinking. We need to become aware of this problem and encourage each other to be more careful with assets by being more careful with our trash.

**Tip**

Many of the topics presented for thought in this chapter and throughout the entire book are just as appropriate in our homes as they are in our offices. This is especially true of our home office computers, networks, and trash!
Most of us are inundated with snail mail at home as well as at work. I have a policy in our home that nothing goes into our trashcan that has any family member's name on it. This requires a little extra effort to destroy a single page of a credit card offer each time I receive one. If it has a name and address on it (obviously everything that arrives at my home does), I destroy that part of the document. Every small thing I can do to protect my family against things like identity theft or credit card fraud helps me sleep at night.

Employee Badges

I know these can be faked, but I still think it's much better to have some form of visible identification worn by every employee at all times. Most of the companies that hired us did not have a policy requiring employees to wear their corporate ID badges all the time. This made our social engineering attempts much easier. Once we were inside the buildings, it was as if everyone just took it for granted we belonged there. Not only were we inside their buildings, but we had also breached their firewalls and intrusion detection systems.

Employees can be somewhat trained to even detect fake ID badges. I was working for a large company that did require employees to always wear their ID badges when they were on company property. This was back in the days when color printers were just starting to show up in homes and offices. I created a fake ID that was intentionally made without any thought of quality control. The first time I wore it into the building instead of my real ID, I suspected I would immediately be stopped and questioned about it. This was a security project, so I was prepared to explain myself. To my initial amazement, I never had to explain anything because it was never questioned. For the next three months, I wore it everywhere and not one person noticed. During one of our security meetings, I told everyone in our group about my little experiment and most people were quite surprised it was never detected.

Part two of my experiment held the most interesting results for me, however. I created a picture showing my two IDs side by side. The fake one was quite obvious when compared with the real one. We began to teach people how to take a closer look at the IDs others were wearing as they walked through our buildings. From that time forward, I only wore my fake ID when I was conducting security awareness training for a group of employees. I was amazed at how many of my friends (who had been through a version of the training) would spot the fake ID as I was
walking past them on the way to the training class. Some would even spot it from ten feet away. These are the same people who (before the class) hadn’t noticed it while sitting 3 feet from me in my office. The lesson here: AWARENESS TRAINING WORKS!

**WARNING**

Tailgating, frequently called piggybacking, is simply following someone into a building after they open the door with an access card or by entering a door code. The “bad guy” will often pretend to be searching for his or her access card while waiting for someone to enter with a legitimate card. If there is no guard at the entrance, the “bad guy” will probably go unchallenged and unnoticed. You really need to think about this one before you decide how you want to solve it. You can’t place a legitimate employee in the position of having to challenge the “bad guy” about identification before letting them in.

The legitimate employee probably didn’t come to work for you to be a security guard. On the other hand, you don’t want “bad guys” just walking into your building. This problem is as old as dirt, but the solutions just keep getting more complex and expensive. Some companies employ cameras that photograph everyone who enters the building. Others are now using biometrics scanners and other high-tech devices. As with everything else in the security field, you need to get a system that is appropriate in cost for what you are trying to protect.

At a minimum, you can make your employees aware of this threat and have them notify their immediate superior that someone followed them in, and then note the time and date of the incident. This same employee awareness session should instruct all employees to display an ID so fellow employees who may not know them don’t think they are “tailgating” as they walk in behind them.

**Shredder Technology Has Changed**

As with everything else these past few high-tech years, shredder technology has changed considerably. Our team had gotten really good at putting strip cut papers back together again. We used to take bags of it back to our office during the test.
Frequently, it was sitting outside in or near a dumpster where we simply picked it up and put it in our vehicle. Most of the time, documents that are strip cut shredded all fall neatly into place in the bag or box where they are stored, waiting to be disposed of. Our team was able to reassemble many of these documents within a few minutes. We would even take a document and paste the strips on a piece of cardboard in the shape of a Christmas tree, spreading the strips out as they were glued to the cardboard. Even with up to an inch between strips, the documents were still easily readable once reassembled. We never even attempted to reconstruct a document that had been sent through a cross cut shredder.

**Tip**

If you have too much invested in your strip cut shredders to replace them, at least consider purchasing some of the small cross cut shredders and place them directly in the offices of people who have especially sensitive documents that should be destroyed. These small cross cut shredders are very inexpensive and durable if you keep them oiled with the special oil available for shredders. I have a small one that cost $39 and it creates a very small particle that would be next to impossible to reassemble. I have tried to wear it out for about six months and it just keeps on working. I’d also recommend encouraging all employees to get one for home use. I believe it is a good policy to shred everything that comes to your home with any family member’s name on it. Once you start doing this, it will become second nature and you will never need to wonder who might see your personal information once it leaves your home. After all, identity theft is on the rise as well.

Outdated but still sensitive documents should also be disposed of securely. When I worked at the Pentagon for the final seven years of my military career, we were required to place certain sensitive (not classified, simply sensitive) documents into a safe containing a burn bag. Burning them would then destroy these items. To this day, I still use a burn bag at home for documents that I need to destroy which are too bulky for my shredder. It’s a great way to clean out the barbecue grill on a cold sunny day. I feel good every time I destroy sensitive personal documents rather than simply throwing them in a trashcan. Left unshredded or unburned, they become possible fuel for the most rapidly growing white-collar crime in the country: identity theft!
Keep an Eye on Corporate or Agency Phonebooks

When we were conducting a test, this was the first thing we went for. Once we got our hands on a corporate directory, the social engineering began. Most corporate phonebooks are laid out in a way that conveniently shows the entire corporate structure as well as the chain of command, building addresses, and department titles. That kind of information also lets us know the order in which to try entering the various buildings, if there were several. Wherever the Human Resources department was located was usually where we went last. Here’s why. As we tried to enter all of the other buildings by simply walking in the door like we belonged there, we were frequently challenged by a receptionist and asked where we were going. Our social engineering answer was always the same. “We were told that this is where Human Resources is located, and we’re here to fill out a job application.” In every case, the receptionist simply sent us in the right direction. We thanked her or him and walked out the door and directly into the building next door to try the same con. The phonebook even gave us the Human Resources manager’s name to drop if we needed to be a little more convincing that we belonged there but were simply lost. It also gave us the names and titles of the rest of the important people in the organization whose names we could drop if we needed to when challenged. In addition to the names in the directories, most contained the physical location and chain of command ranking for the most important person in each department. It was often their offices, file cabinets, and trashcans that we spent the most time in during our nightly visits.

Employee awareness of how important a corporate directory is will help greatly with this one. Old directories are still quite accurate especially regarding buildings and department locations. They should be burned or shredded rather than simply thrown into the dumpster.

If paper directories can be eliminated all together, that would even make our job a little tougher. Everything you do to make it a little harder for the bad guys will make you a less likely target—they’re looking for an easy mark. Online directories are better only if you don’t let the social engineers get into your building. Once we were inside, we began looking for a monitor with the infamous sticky pad note on the side listing the person’s login ID and password. Once we logged on to the network as them, we could usually get to an online company directory if there was one.

Let me address one additional countermeasure while I’m on the subject of the login ID and password that’s been written down and attached to the monitor or placed under the keyboard. Maybe that doesn’t happen where you work, but we
found at least one person who had done this on every job we were hired to do. There is another reason we like to use someone else’s login ID and password to get onto their networks. If we are able to do that, not only are we on their network on the inside of any firewall, but everything we do will show up in some log as being done by the person who let us log in as them. Many larger companies now employ at least some form of two-part authentication using either biometrics or some type of handheld authenticating device to attain two-part authentication. Fortunately, some forms of biometric access control are becoming very reasonable in price. Everything you do in the way of authentication will greatly reduce your vulnerability in this form of instant identity theft.

**Tailgating**

This was one of our most successful entry techniques, regardless of the security procedures at the building. For some reason, people in the outside smoking areas didn’t ever question our being there and eventually walking in right behind one of them as they went back to work. We found that many corporations had good security at their main entrance points, but were lacking at other entry and exit points. We were able to gain access on several occasions through parking deck or garage entry points that required card access. We would simply follow someone who was headed to the door and walk in behind him or her as we were pretending to search for our access cards that didn’t exist.

**WARNING**

Here again, employee-wide awareness training and a strong security policy can go a long way in preventing this type of an entry. These outside break, lunch, and smoking areas are frequently places where there are no security guards or receptionists trained to ask for proper ID as someone passes through the door. As mentioned earlier, having every employee wear an ID badge would make this type of entry a little more difficult should someone try to walk in without an ID.

The countermeasures for this vulnerability really aren’t as simple as we might think. Most employees entering a building aren’t security people. They are simply trying to get back to work. Even though someone entering a building using the tailgating or piggyback method should be challenged, challenging them is an uncomfortable situation for most people. Unless there is a strong corporate policy requiring all employees to challenge anyone they can’t identify, this is a difficult problem to deal with. At an absolute minimum, employees
Building Operations:
Cleaning Crew Awareness

I can’t emphasize enough the need to train all of your second- and third-shift employees, and especially your janitorial services people, about the threats of social engineering. Obviously, pre-employment screening, and possibly bonding, is essential for any outside firm you allow inside your buildings at any time. This is especially true for building access outside the normal 8 to 5 Monday through Friday standard work schedule. Frequently, these people have access to the master keys for a large section of the building and sometimes the entire building. They need awareness training to better prevent them from becoming victims of bad-guy social engineers who would like to borrow their keys for a minute or get them to open a certain room.

This team should also immediately know whom to contact should they see anything suspicious that should be reported. If there is no immediate supervisor on duty during the evening or night shifts, everyone on that shift should know how to quickly contact their security forces. It can be very dangerous for them to approach a stranger themselves in an attempt to get them to leave.

This suggestion may not seem to fit in the context of this book, but let me mention it anyway. There is another very good reason to train your janitorial team (at least the team supervisors) to be extra watchful during the evening and night shift work hours. I have been teaching bomb recognition classes for the past ten years. These same social engineering skills and physical building penetration methods could apply in any situation where the collective “bad guys” are trying to get into your building. The eyes and ears of the people who work in your building every day are critical when it comes to detecting anything, or anyone unusual in the vicinity of the building. Bomb recognition training for key individuals and as well as having an effective bomb incident plan are other countermeasures that can be employed to considerable effect.
Security Alert...

Bomb Threats in Chicago

This is a good time for a little side story that will let you see how the many risks, threats, vulnerabilities, and countermeasures overlay in the worlds of physical and technical security.

Several years ago, I received a call from a friend from the Chicago area asking for help. He said his company had office locations in several cities throughout the country, and one office out of the country. A series of bomb threats called into their corporate headquarters were causing them to lose sleep. They just wanted our team's suggestions regarding what they should do about it. This meant a trip to Chicago for us in February. (For the warm-blooded person from the sunny south that I am, it was like taking a trip to Iceland in mid-winter.) We went anyway.

Prior to going, I decided to look on the Internet to see if I could find out anything about the company. It could also provide a hint as to why someone would call in these bomb threats (that fortunately were only threats, so far).

The company flew in their senior managers from around the country and we suggested their corporate attorneys and risk managers attend the training as well. They would learn everything they wanted to know, but were afraid to ask about bombs and bomb threats.

We arrived a day early and asked if they would like for us to take a look around their corporate headquarters building to see if we saw any glaring physical vulnerabilities that might allow someone to easily place a bomb in their building, or in a spot nearby outside. The outer perimeter was about as close to perfect as I had ever seen in a building of that size. As we were looking at the various locations from the inside, my eyes kept being drawn to their newly installed access control system. Each employee had been issued an ID card that would allow him or her to enter certain doors at specific times of the day. The system also kept track of the times they entered and left the building. It was impressive.

My fellow team member gave me a strange “you've done it now” kind of look when I said that a simple metal coat hanger might be able to compromise the entire system. I was about to be put to the test as we approached the next set of outside access doors in that part of the building. The person who had hired us stood there with a metal coat hanger and handed it to me.

Keep in mind, we were walking around inside the nicely heated building without our coats. On the other side of the doors, which I would now attempt to open from the outside with the coat hanger, it was still Iceland in February.

Continued
I politely said I would go outside (without my coat) and try for a few minutes. All I asked was that if I started turning blue, to please “open the door from the inside and let me back in.”

In the end, my request proved necessary. I was back inside in less than 30 seconds and everyone was standing there with a deer-in-the-headlights look as I calmly walked through the $250,000 security system with no indication I had ever been there. This was not the first time I had seen this issue with an improperly adjusted access control system. The system was one that detected motion from the inside, thus automatically unlocking the door as soon as it detected someone moving towards it. I noticed it detected us walking past the door from a considerable distance away. It was just too sensitive. I also noticed that the locking mechanism opened only one of a pair of double doors and that the motion sensor was mounted dead center between the double doors. The only thing protecting the opening between the double doors was a thin piece of weather-stripping. While I was standing outside, quickly freezing to death, it was a simple matter of taking my thin metal coat hanger and sliding it between the two doors while rapidly moving it up and down. Within seconds, I heard the familiar “click” I was hoping for. The security system thought I was inside because that’s where it saw the motion of my coat hanger.

For another insight into this vulnerability, be sure to read Johnny Long’s chapter as well.

All of the senior managers, attorneys, risk managers, and security team members were in a training room the following morning for their day of Bomb Threat Training. I opened the meeting by letting them know that this was most likely a low probability threat, but that they were smart to decide ahead of time to learn as much as they could about what they should do about these threats. We were going to spend the rest of the day learning about bombs, bomb threats, bombs in buildings, bombs outside of buildings, and all kinds of other scary things. It was going to be a fun day.

As I was finishing up my introduction, I walked around the room and placed a small packet of one to three pages in front of four of their most important people. As the four targeted people started to look through the papers placed in front of them, I simply stated that this was their high probability threat and something they needed to address immediately in our opinion. The papers contained just about everything we would ever need to know about these people. Where they lived, how they most likely traveled to work, where they went to college, where their children went to school, and much more. All of it was gained from a few social engineering phone calls and about an hour searching the Internet for information about them. Much of the information about these people (and possibly about you) was out on the Internet. It’s not easy, but these people-type search engines all have an opt-out capability so you have your name and contact information removed from their databases. Just type the words “people search engines” into www.google.com for the most recent list of these services. You should input your name into

www.syngress.com
some of them to see what information is out there about you. You’ll likely be surprised how many times your name pops up.

Spot Check Those Drop Ceilings

On several occasions, we used our social engineering skills to get into buildings and then install a sniffer in the telecommunications hub for that floor. I recommend all companies have their building maintenance teams perform a spot check above all suspended ceilings at least twice each year. We have been amazed at some of the things we found up there while we were conducting the penetration test. You may even stumble into a security vulnerability you weren’t even aware of.

This suggestion would also be one I would make if considering places to hide things like bombs. We walk under drop ceilings day after day and normally have no reason to think about what might be up there. Usually, there is at least a foot of clearance between the grid work holding the drop ceiling in place and the ceiling itself. I have seen as much as three feet of clearance. You may be amazed at what you find hidden up there (hopefully, it isn’t ticking).

Check for Keystroke Readers

Some of our favorite tools are the software, and newer hardware versions, for keystroke readers. These can make a good social engineer’s job a lot easier. If we wanted to find out what a certain individual in the company was doing on their computer during a certain timeframe, we would install a keystroke reader on their workstation on one visit and retrieve the results on a second visit.

By far, the most effective keystroke loggers we have used are the Key Ghost hardware loggers being sold as security devices (www.keyghost.com). When these are installed between the keyboard of a workstation and the keyboard socket on the back of the computer, to the casual observer they look like they belong there. The one we used looked like the induction coils seen on some of the older parallel printer cables. It just doesn’t look like anything you need to worry about.

However, if you didn’t put it there, you better be worried! It’s logging every single keystroke you type in.

The version we used would hold about 500,000 characters or half a megabyte. That might not sound like much, but just consider that the Word document that eventually became this entire chapter would take up about 20,000 characters (16,000 characters for the text and about 4,000 backspace key strokes to correct all of my typing errors). That would only be about 4 percent of its capability. By the way, those backspace keys would show up as ASCII characters (control H for you techies) as
would any other non-printing character entered as part of a password or whatever. It
only records keystrokes, so it holds a lot more than you might think. We’ve left them
connected to target computers for up to three weeks and still only filled about 80
percent of their capacity.

Here’s something else to consider if you feel safer entering information into
your Web browser over a secure socket connection (https). The encryption happens
between your browser and the server that is receiving your sensitive information
over the Internet. That’s a good thing if you’re entering your credit card number or
bank account access information. But here’s the problem with that warm fuzzy. The
keystroke reader is reading your keystrokes before they get to your browser.
Everything will be in the clear when someone (hopefully only you) looks at the data
your keystroke reader collected.

How do you know if you have one connected to your workstation or home
computer? You don’t unless you physically look back in the rat’s nest behind most
computers and see if anything looks strange. Unless you know what they look like, it
probably won’t appear strange to you even if you do see one. I pass one around for
people to see at all of my security training classes. Statistically, I’ve read that people
are 27 times more likely to remember something if they are able to see it and hold
it. I usually ask my attendees to raise their hands if they’ve never seen one. Almost
every time, more than half of the hands go up. How can you defend yourself against
something you don’t even know exists? (Another subtle hint for more awareness
training.)

Here’s a quick awareness training class using one of my workstations as the target
computer. The picture in Figure 1.1 shows the workstation in a minimum configur-
 ration with only a monitor, mouse, power cord, and keyboard connected to the
motherboard. Take a look at that little bulge about three inches from the end of the
cable that goes to the monitor. It’s the only cable that has a bulge of the four that
you see. That’s an induction coil and you may see one or more on cables found
behind most workstations.
Let's take a look at this same workstation after I have installed my keystroke reader between the keyboard and the motherboard socket where the keyboard was connected (see Figure 1.2). Of the two cables in the center next to each other, the keyboard cable is the one on the right.
Now what do we see when you look back there? The keystroke reader looks like a second induction coil and would be very hard to detect if you didn’t know what one looked like. I didn’t try very hard to hide it, and normally there are more wires back there than this. There is no way the computer would know it is there. It uses virtually no power, and doesn’t require any software be installed to make it work. When I finally remove it and take it back to check out the internal log, the computer (or you) would never know it was gone again.

The keystroke reader is an excellent security device if you suspect someone is using your computer when you’re not there, and is sold primarily for that purpose. It’s a wonderful piece of equipment… as long as you know it’s there.

Check Those Phone Closets

If your office is in a rented space, or in a multitenant building, it’s a good idea to have someone perform a thorough check of your hardwiring for the phone lines. You don’t know who was there before you were, and old wiring sometimes isn’t removed when new tenants move in. On more than one occasion, our teams found old phone cable wiring still in place and being used in an inappropriate manner by inside employees. While we are on the subject, Techno Security also comes into play when considering the corporate PBX (or Private Branch Exchange), which is the internal phone company for larger corporations. It may still have a modem for remote maintenance needs, and the phone number for that modem may be written on the wall near the modem. We found many of the PBXs we “visited” to be very social engineering friendly.

Remove a Few Door Signs

It always amazed us to see rooms that had a sign over them saying Computer Room or Phone Closet. Obviously, the people who work there know where it is, and there is no reason for anyone else to know what’s in there. It’s all right for the room to have a number on the door that building maintenance would understand, but there is little reason to make it so easy for the bad guys to know where their best target is on that floor. This may sound like I’m getting a little too picky, but I’m not. The more difficult you make it for people who don’t have a need to know about these critical rooms, the more secure you will be.
Tip

If you are going to have high-security locks on any doors in your building, dedicated computer rooms and phone closets would be high on my list of rooms needing the most secure locking mechanisms.

Review Video Security Logs

Normally, after we have completed our mission and have taken all of the “evidence that we have been there” out to our vehicle, we would reenter the building and try to be seen by the building security cameras we knew were there. Hopefully, there were some we didn’t know about. We would even jump up and down waving our arms just to see if anyone would actually report us. As far as we know, we were never reported as being seen on the cameras’ tapes. One of three things must have happened. Either the cameras weren’t working (unlikely), or the people looking at the playback of the video missed seeing us on the tape (probably unlikely) or they were never looked at (most likely). I’d recommend that someone in the company periodically test this process. If there were internal auditors in the company, this would be a good audit step. That big expensive surveillance system is worthless if whatever is captured on tape is never seen by a human who can do something about it.

This is another area where I believe the people responsible for the systems’ techno security need to talk with those responsible for physical security. Cameras and lights have always been excellent countermeasures in and around buildings and homes. They scream “go find an easier target” to the bad guys. Some areas may require additional cameras to help improve the security of critical areas or rooms. The team responsible for overall physical security might not know of these places unless you tell them. They may already be monitoring areas you aren’t aware of, which could help you if an incident occurs.

The reason I mentioned homes several times throughout this chapter is because they are another soft spot when it comes to physical penetrations or social engineering. Many people now do much of their work from home on workstations using high-speed Internet connections. Personally, I employ as much physical security at my home office as at every other office I have worked. The technology associated with home security products has increased significantly, while the prices for that security have dropped, along with the cost of the latest computers.

I recently installed a number of digitally controlled security cameras around the perimeter of my home, as well as motion-activated security lights in all approach
areas. This may sound a little paranoid, but I know that I am much more protected than most of my neighbors, and my family feels safe knowing it would be difficult to commit any crime on our property without someone knowing about it. The cameras are also motion activated, so the only thing I see is activity detected by the software. With the rapid advances in technology, these kinds of sophisticated security systems are very affordable and powerful.

Motion-Sensing Lights

Most of our social engineering–based inside penetration tests would have been much less successful if the companies that hired us had motion-sensing light controls installed in every office throughout their buildings. These same sensors then turn the lights off after a pre-set time once the last person leaves the room.

Every penetration test we were hired to conduct gave us several opportune buildings to enter, and every one had at least a few lights on all night long. While conducting our initial surveillance, that was one of the first things we noted. Are there lights left on at night, and if so, are they the same lights every night? In most cases, in a building with, say, 15 floors, six or eight lights would be left on. Our assumption was that whoever was assigned to that office was either still there, or they forgot to turn the light off when they left. Either way, it helped us significantly. If a random number of lights were left on each night, the security forces would not have an easy way of determining if everything was “normal” at any given time.

As they patrolled from the outside (we watched them do this from the outside, and also from the inside once we got into the building), they really had no reference for what was a normal building profile. As we became bolder towards the end of a penetration test, we would even turn certain lights on just to see if security would become suspicious of this activity. No one ever did.

Several of the buildings we penetrated didn’t have anyone working in them at night. If motion-sensing lights had been used throughout these buildings, we would have looked for softer targets. If we had entered a room in a completely dark building, the light coming on would have been very abnormal for any security team member who saw it.

There is another good reason to install these sensors. Over time, the energy saved by having the lights automatically turn off when no one needed them could eventually pay for the cost of the sensor.

Check All Locks for Proper Operation

During each penetration test, we found at least one lock (either interior or exterior) in the building that wasn’t functioning properly. This provided us with easy access to
buildings and rooms that we shouldn’t have been able to get through so easily. If employees are trained for just a few minutes on how to check if the locks on the doors they use every day are working properly, this vulnerability can be all but eliminated. Building maintenance teams should also take a close look at all locks at least twice each year. Slightly misaligned strikes on the doorframes are the most common problem found. This is a serious problem because it defeats the purpose of the lock’s dead bolt. It takes me less than a second with my trusty finger nail file to see if a particular lock has this problem. If it does, I’ll know (and have the door opened) instantly.

**Warning**

Don’t forget to check those locks and doors at home. We also recommend that lock combinations (keys) be changed immediately after occupying a new home, or after moving into a home that was owned by someone else. Keys are easy to duplicate, and you have no way of knowing how many copies are already out there, even for a brand new home. I’d also recommend changing the codes to your garage door openers as well, which is very easy to do with most modern openers.

If you have a garage door opener installed, do not leave it set to the default code (frequently 000000 or something very generic). This could make you vulnerable to another form of wardriving where the bad guys simply drive around neighborhoods with generic openers trying to see if any doors open as they drive past. This gives them a nice potential target for a future break-in. Also, many houses that have house alarms don’t have an alarm on their garage door. Even worse, the keypad for turning the house alarm on or off is frequently located next to the garage entrance inside the house.

If you ever find your garage door opened and you didn’t open it, I’d recommend immediately changing the door opener (and receiver) code.

The Elephant Burial Ground

I’ve been making a simple statement at presentations for the past ten years: “A new computer is a wonderful thing, but as soon as you buy it, it’s already obsolete.” Technology continues to change at a rate that few of us even notice. My statement
isn’t meant to be negative in any way. It’s just that the computer is doing exactly what those new calculators did 35 years ago. They simply get faster, better, and cheaper as soon as you walk out the store’s door. I’m not suggesting you don’t buy the new (soon to be old) computer, you just must realize you will likely need a new one in two years.

What happens when that “elephant” you purchased a few years ago finally dies or becomes too old to do any work for you? I’ll bet it gets moved to your elephant burial ground with the rest of the electronic equipment that still looks new and valuable but isn’t fast enough to keep up anymore. You can’t simply put it out for the trash man to pick up, so there it sits, sometimes for years.

This burial ground was a prime target for our penetration teams as we conducted vulnerability tests inside our clients’ buildings. We frequently used our social engineering skills to find out where the old computers were stored. If it was in a locked room, we would find a way to either get someone to open the door for us, or we would use our lock picks or pick gun to open the door.

Figure 1.3 shows pick sets similar to the one I’ve owned for over 30 years, while Figure 1.4 shows a pick gun comparable to mine. It doesn’t take a lot of practice to learn how to use the latter. If you are thinking about running out and buying some of these tools, please be sure to read the warning I have included below the pictures. I don’t want to have to include you in a future war story about what NOT to do with lock picking equipment.

Figure 1.3 Examples of Lock Pick Sets
Figure 1.4 Example of a Pick Gun

WARNING

Possessing lock-picking equipment is illegal in some states. If you intend to pursue lock picking as a hobby, or as a part of conducting your own “official” penetration test, you still need to be sure you are not breaking the law in any way by making or using these tools. As with almost any subject today, there is a wealth of information on the legal issues associated with lock-picking, and which are available on www.google.com by entering “are lock picking tools legal to own,” or something similar.

The “bad guys” I collectively refer to throughout this chapter most likely won’t care if they are legal or not. But you should!

Once we found a room that contained some outdated equipment, and so knew we were going to leave with some very valuable intellectual property. All we did was open a few computer cases, remove the hard drives, and neatly close the case back up. How valuable was the information on that drive, and how soon would you know it was missing from the elephant burial ground?
Most likely, you would never know the disk drives are gone. Our experience has been that these older computers are seldom powered on again by the organization that owned them. They may get powered on by whoever eventually winds up with them at some junk auction or thrift store where they were donated. If they sit in any onsite location for any length of time, the chances of anyone ever knowing that the entire computer is missing, much less the hard drive itself, are very slim. For the most part, it could remain an undetectable crime.

How valuable was the information on the old drive? Our experience has been that about 80 percent of the information on the old drive may still be of value to the “bad guys.” If you think through the process of how that computer wound up in the burial ground, you will see what I mean. If the data on the old drive were properly backed up as a part of your disaster recovery plan, then it would most likely be restored to the new computer prior to retiring the old one. As soon as everything looked fine on the new computer, the old one may never be powered up again.

Technical issues are associated with each of the processes just described, but I didn’t go into that detail here. Here’s the bottom line from my experience with these old drives. If they weren’t properly whipped clean, and if the drive itself was operational, we were able to get to the data on them with no problem.

**Tip**

Old disk drives will be an area of concern for years to come. Terabyte drives will soon be available at stores like Office Depot for anyone to purchase. Less than ten years ago, I was thrilled to be able to purchase a 200MB disk drive for $200. I was the first person in my circle of friends to own a drive of this size, and all for a mere $1 per megabyte. Today, 200GB disk drives can be found for as cheap as $50, after rebates. That’s about 25 cents per gigabyte, which means that the same $1 per megabyte (actually worth less today) would buy me 4 GB, or 4,000 times as much storage space for the same dollar spent.

The tip here is to be careful with those old disk drives. This applies to the computers at home as well as at the office. Much valuable data is on them, and the risk escalates as the storage capacity of every drive climbs rapidly each year.

Figure 1.5 shows a destroyed disk drive, and Figure 1.6 shows the machine that destroyed it. The following is the URL of the only company I know that offers complete destruction of obsolete hard drives: www.edrsolutions.com.
Figure 1.5 A Destroyed Disk Drive

Figure 1.6 The Machine That Destroyed It...
Internal Auditors Are Your Friend

Just about everything I have mentioned in this chapter would make a good spot check audit point for an internal auditor. Someone on the good-guy side of the fence needs to check for these possible vulnerabilities and insure that the proper countermeasures are employed before they are exploited and become security incidents.

My experience with auditors over the years has been that things usually happen once they have made a suggestion to improve an area of concern. Many larger corporations have information system auditors who are primarily responsible for looking after the company’s technical world. It’s a lot to keep up with. Most mid-sized corporations have internal auditors who are responsible for IS in addition to all their auditing tasks.

Always Be Slightly Suspicious

The number one countermeasure for social engineering is to be a little more suspicious than we normally are as friendly, trusting Americans. This holds true for social engineering attempts whether by way of a phone call or a visit from an amicable salesman. We all just need to be a little more aware of what is going on around us and those persons who might be pretending to be something they aren’t.

Unfortunately, this is a difficult countermeasure to keep ongoing. Still, we should not become complacent in this area. If we do, it will make life much easier for future bad guys. This and most of the countermeasures suggested in this chapter will help mitigate all of these threats.

Get Every Employee Involved

I’ve been saying this over and over for close to two decades now. I don’t care what kinds of sophisticated security devices are employed for physical access control or network access control with intrusion detection, firewalls, incident response, and so on, there will always be a large hole in a security plan if it doesn’t get all of its employees involved with the protection process.

Social Engineering Awareness: A War Story

The phone rang at nine o’clock in the evening way back in the late 1980s. It was our national technical support group on the line. The caller said he had spoken to the day-shift supervisor, and that he needed to run a test by having us log in to our
maintenance port while he was on the line. This was a UNIX-based operating system, and back then we always logged in as root. That was a very standard system administrator login ID and there was no need to guess it. What this social engineer needed was the password. In very official sounding language, he managed to convince our evening-shift computer operator that he was going to run a test to check the security of the password as the operator was entering it. The passwords themselves don’t appear on the screen (echo is turned off, for you techies out there) but the characters are sent in the clear. The person on the other end of the line said that something wasn’t working correctly. He couldn’t see the password coming in to him (obviously, it wasn’t really going in to him anyway). He then asked our operator to try again. The second time the operator had the same results. The pretend technical support group person began to sound a little frustrated. He finally said, “What password are you entering? I’ll try it from this end.” The unsuspecting social engineering victim was then told that this fake support person would get back to him when the problem was corrected. Obviously, he never heard from this person again.

Unfortunately, this was before our pre-awareness days, and the caller got what he was after. He had done his homework and come up with just enough information to sound “official” and catch our evening person off-guard. In a story with a happier ending, the same thing happened two years later, but we were completely ready for it this time. Our employee wide awareness program was paying off.

This process of calling and getting information from an unsuspecting victim over the phone is a form of remote “social engineering” in the “bad guy” circles. It’s quite effective when used against an unsuspecting victim. Making sure every employee (especially everyone who answers the company phones) aware of this threat is your only defense against it. By asking questions back to any suspicious caller, you will drive away most of them. Ask for a number to call them back on. That doesn’t guarantee anything, but I’ve heard a few clicks as the phone is hung up after I’ve asked for a number.

At a minimum, be aware of this highly probable threat and decide ahead of time what kinds of questions will, and will not, be answered about the company over the phone. This is an area where employees can get involved. At a monthly meeting, a “Social Engineering Attack Drill” can be staged. I’ve never been fond of role-playing sessions, but this is one area where it could be both fun and effective. The incoming caller can be engaged in industrial espionage, competitive spying, intentional destruction, just plain curiosity, or any number of things. If the team representing the company prepares for the questions that might be asked over the phone, there is a good chance they will hit on most of the questions the real social engineers will ask.

Once our employees were made aware of this threat, their antennas went up as soon as a call came in that was even the slightest bit strange. Yours will, too.
don’t want to be insulting or rude to anyone who calls into your business. That’s just not good for customer relations, and most businesses need customers to call them every now and then. You can be firm and alert sounding while still being nice to the caller. Gently let them know you are not about to give out any unnecessary information over the phone. If they are legitimate callers, they will come to appreciate your protection of company information. It may even be information about them, and who wouldn’t want that protected?

Other good things start to happen as an awareness program filters through an organization. As employees learn more about the reasons for tighter security (such as keeping the company, and their jobs, from going down the tubes), they will tend to stop trying to circumvent existing security measures.

I learned something else from the seminars I gave years ago: employees are very much interested in helping with the overall security posture of their company. I started receiving copies of newspaper articles from former attendees, in case I hadn’t seen them. I was starting to be made aware by my students, and it was rewarding for all of us. This internal network was starting to grow and security was becoming a challenge instead of a chore.

Something else I started took off as well as my homegrown awareness seminars: my security awareness posters. I wanted to make posters that were effective, eye catching, and cheap. My self-imposed criteria also demanded that they be easily reproducible on a standard copy machine. With those thoughts in mind, I sat down with a clipart book and let my imagination do the rest. After two hours, I had enough clipart drawings, and clever sayings to go with them, to design posters for the next two years. I sent out a new poster every three months to a select group of people. It didn’t take long for others to call and want to be added to my list for receiving the next poster. Some people started to collect them and line them up along their walls.

After I spent six months sending these posters to whoever wanted one, a stranger I had never seen before in our building visited me. He came to my desk, said hello, and introduced himself as a corporate external auditor who was auditing a group in our building. I knew and worked with a number of our own internal auditors, but this was the first real live external auditor I had ever met. He made me feel at ease very quickly though by telling me he wanted to meet with the person who designed the posters. They were so simple, yet so effective, he wanted to take them back to his company. I said thanks and to help himself.

Here’s a quick example of what I did for one of the posters. Using an interesting clipart picture of someone sitting in front of a computer, which included a caption that read “Take Advantage of Today’s Technology,” I simply added four words, creating what became my most popular poster. Below the phrase “Take Advantage of
Today’s Technology” I added, in large print, “THE BAD GUYS WILL!” It was that simple.

With the clipart available today, you can come up with some excellent ideas very quickly. I even started a contest to see who could submit the most interesting poster suggestions for the following year’s posters, even awarding prizes to the winners. All it takes is a little imagination and off you go. Have fun!

As the demand for my internal security awareness seminars increased, I was faced with an ever-growing problem. More and more groups wanted to see the presentation, and I couldn’t possibly get to all of them. After all, giving these seminars wasn’t even part of what my immediate group was supposed to do. My next step was to recommend a video be prepared and used by all of the groups that I couldn’t get to. The initial reaction was that it could be too expensive. A studio quality video can cost over $1,000 per minute to create. Even a 30-minute video would be out of the operating budget for most groups at $30,000. That wasn’t what I had in mind.

Something much less elaborate was what I was suggesting, and with the help of a friend with a video camera, it was created in less than two hours for just about zero cost. Just to see how it would look, we ran the camera during an entire 30-minute session that I presented to a small group. We then created a video of nothing but the slides that were used. The remaining hour was spent editing the two videos together. Our intent was to try this a few times until we got it right. We were trying to come up with something that would be cheap (the most important part at the time) and effective. We had no idea how successful our first attempt would become. Over 100 copies of it were sent all over the company, and most copies were shown a number of times throughout the next year to insure everyone had a chance to see it. As far as I know, it is still being shown.

I’ve shared all of this here for a reason. If I can do it, so can you or someone else in your company. I learned that homegrown videos are quite popular. In some ways, they gain a certain additional credibility if they are “real life” and not overly commercial. The equipment to create them is getting more sophisticated and less expensive all the time. If you try this yourself, I think you will be pleasantly surprised at the outcome.

There was someone else in the company that was pleasantly surprised by my seminars, posters, and videos: our internal auditors and attorneys. It was going a long way towards giving them plenty of good “Due Diligence” examples of what we as a company were doing to prevent computer security violations, both internal and external. Along those lines, I always encourage people who either attend a seminar, or view a video to make a note that they have had some security awareness training. As people all over the company do that, there will be an ever-growing population that is proof of the company’s “Due Diligence” intent.
To help with this, I created a “Certificate of Attendance” that I send to everyone who attended one of my seminars. These are another low-cost and highly effective “Due Diligence” statement. Even though they are inexpensive to create, they are very nice and frameable. In fact, as I traveled around, I saw a number of them hanging near the desks of former attendees. You could create your own company certificate as easily as I did. All that you need is some good certificate stock (blank paper), a word processor, and a laser printer. After you experiment with the fonts and word sizes, you can keep a template that only needs to have the names mail-merged to create the documents. They will look as good as any you’ll ever see, and you will have one more thing that the internal auditors will love to see hanging on the walls.

There is one final thing that an effective awareness program will help your company with, but I always dislike mentioning it. It will help deter “inside” activity. Unfortunately, every statistic I have ever read on the probability of security violations has pointed towards the “inside” of companies. (For more on this threat, read Dr. Eric Cole’s book by Syngress titled *Insider Threat.*

Security Alert...

**Inside Threats**

Experts estimate that over 80 percent of all breaches and problems come from someone inside the company. I never believed that until I started working with various law enforcement groups. Here’s where awareness can even help deter that kind of activity. If your program is presented to all employees, obviously any potential inside “bad guys” will be sitting there as well. That’s just fine. You won’t be telling them anything they don’t already know about how to get into your computers. You will be informing them that all the employees are now aware of a number of security issues and that their chances of getting caught in the act are far greater now that the corporate awareness level has been raised.

How long will you and your company have to continue your awareness campaign? Probably for as long as you continue to work, and computers continue to exist. I’m far from a doomsday person, but I do see this computer security issue as having the potential to be a major concern as we move deeper into the twenty-first century. There will always be those who find it an exciting challenge to see what they can get into in cyberspace.
Answer to the Riddle

The two coins are a nickel and a quarter. I know what you’re thinking. I said that one of the coins was not a nickel. That’s true. One of the coins is a quarter. The other one is a nickel.

Summary

I’ve thrown a lot at you in this combination of risks, threats, vulnerabilities, and countermeasures associated with social engineering. What I have tried to address in this brief chapter is what I consider the low-hanging fruit that the bad guys are very aware of. Most of the vulnerabilities mentioned are fairly easy to fix once you know about them. Most of you who read this book won’t be responsible for correcting many of them, but you might be able to get this book to someone in your organization who can.

Security will always be a long-term team effort. This is true for every company and every home. If you have a computer in your home and you access the Internet to pay your bills or check your bank statement, you need to consider security every time you do so. Even though we live in a technical world that will do nothing but get more technical, we can’t forget about physical security at home and work. If you become a victim of identity theft, you will spend about two years getting your financial life back in order. Prevention is your absolute best countermeasure for most, if not all, of these possible threats.

Thanks for reading all of my keystrokes as I put my 30 years of lessons learned on paper.

Stay safe out there!