Jack Wiles, (PPS, IAM, IEM) is a Security Professional with over 30 years experience in security related fields. This includes computer security, disaster recovery and physical security. He is a professional member of the National Speakers Association and has trained federal agents, corporate attorneys and internal auditors on a number of computer crime related topics. He is a pioneer in presenting on a number of subjects that are now being labeled ‘Homeland Security’ topics. Well over 10,000 people have attended one or more of his presentations since 1988. Jack is also a co-founder and President of TheTrainingCo., producers of the Annual Techno Security Conferences and the popular Techno Forensics conferences. 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, Department of Justice, The Department of Defense and numerous members of High-Tech Crime units. He was also appointed as the first President of the North Carolina InfraGard chapter that is now one of the largest chapters in the country. He is also a founding member and ‘official’ MC of the US 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. He recently retired from the U.S. Army Reserves as a lieutenant colonel and was assigned directly to the Pentagon for the final seven years of his career. In his spare time, he has been a senior contributing editor for several local, national and international magazines.
Introduction

Please don’t let my opening chapter’s title make you think that I’m starting this book off in a negative light. Believe me, I’m not. There are many positive things we can all do to help secure our most critical applications and resources. Some of the things I will discuss in this chapter have been on my mind since the mid ’70s. I believe it’s time that I put them in writing, and present my thoughts on what I believe could be the biggest potential hole in any security plan: Physical Security!

This chapter (as well as the rest of the book) isn’t meant to be read as a complete story from beginning to end. I’m writing it as a collection of experiences and learned lessons from 30-plus years of working in the fields of physical and technical security. Some of the subject matter in this chapter is partially covered in chapters of mine in our other Techno Security’s Guide series of books. I do believe that the readers of this book will most likely come from a different group of specialists than the readers of our other books. Throughout the book, you will also notice that several of our authors will address similar topics from their perspective and experience level. A good example of this will be the discussion of locks, keys, and bypass methods. I first became a locksmith in 1970 and worked in a locksmith shop for several years learning the trade. I’ll share a lot of my thoughts on this critical subject throughout my chapter. Unlike the technical world where most things sitting on your desk are already obsolete, many of the locks used in our buildings (and in our homes) haven’t changed at all in many, many years. Most of what I learned in the early ’70s is still very applicable today when it comes to the common locks found on about 95 percent of the doors on the planet.

The reason that I rambled a little about locks at the beginning of my chapter is to let you know that some of the other authors in this book will have their own opinions and suggestions regarding these critical pieces of hardware. Marc Weber Tobias wrote one of our chapters, where he goes into great detail on High Security Locks and their possible vulnerabilities. Without question, Marc is considered one of the most gifted experts in the world today in understanding and researching the security offered by many types of locks. We are honored to have his work in this book. Be sure to read his chapter carefully, because some of the locks you’re relying on to protect critical information and equipment might not be as secure as you think.

I’ll be addressing a number of risks, threats, and countermeasures (there’s that risk management talk again) throughout this chapter. Let’s go ahead and get my thoughts on locks out there as my first in-depth topic on physical security.
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 that it’s not very often. This can be an expensive process. Recently, I walked into a public rest room 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 that the janitor had just filled the towel rack and left his keys hanging there. Should they fall into the wrong hands, the person could own the building.

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 that 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 ‘70s 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 don’t suspect that many “casual” social engineers use them. They require a lot of that “practice, practice, and more practice” stuff that’s required for any social engineering skill. The availability of these devices for anyone to purchase is something that corporate security specialists must 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. It is very seldom a good idea to have one key that opens everything in the building. It may be convenient for certain things, but it creates 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 Medico 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/her policy regarding the security of the master keys. It will let them know you are aware that 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 additional 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 the evening and night shifts. 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 that 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 people are gone. They spend some time in just about every room in the building each week. If you train no one else in your company, these people must be well trained on how they can help. They should be made aware of your security policies and what they can 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.

**Check All Locks for Proper Operation**

On every one of our penetration tests, 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 to see if the locks on the doors that 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 that we find. This is a serious problem, in that it defeats
the purpose of the dead bolt feature of the lock. 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.

**Tip**
Don’t forget to check those locks and doors at home. We also recommend that the 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 in a brand new home. I’d also recommend changing the codes to your garage door openers as well. This is a very easy thing to do for most modern openers.

**Warning**
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 war driving where the bad guys simply drive around neighborhoods with generic openers trying to see if any doors begin to open as they drive past. This gives them a very nice potential future target for a break-in later. Also, many houses that have whole house alarms do not have the garage door alarmed. The keypad for turning the alarm on or off for the house is frequently located in the garage.

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.

### A Little More about Locks and Lock Picking

Locks have fascinated me for almost 40 years now. In many ways, they are the hardware versions of the passwords and authentication devices that we use to gain access to our computers. They are also what I like to call the low-hanging-fruit of your perimeter security. Unfortunately, many times, they are the place where we spend the least amount of money. I’m going to try to convince you to spend a little more for a whole lot more protection when selecting locks for your office or home.
In preparation for this part of my chapter, I visited several chain stores just as school opened to watch people. Johnny and I both do a lot of people watching while we are out and about. It’s fascinating. As I was looking around at the locks available in different stores, I watched as several people came over to the area and quickly picked up a lock or two for school. Most of them chose a Master brand combination lock that has been a standard for decades. That didn’t surprise me. I also watched as several people purchased padlocks with keys. What every one of them did wasn’t a surprise either: They purchased the CHEAPEST lock they could find. I watched this over and over again. Little do they realize that they got what they paid for.

Most of them picked up either a warded padlock, or a cheap pin tumbler padlock, none of which costs more than $5. These locks looked as strong as the better locks on the outside, but anyone who knows even a little about locks knows that these cheap locks aren’t even going to keep the honest people honest. How about a quick lock awareness war story to give you an example of how easily the wrong type of lock can be bypassed:

### Case Study

**A Lock Awareness War Story**

Our penetration team had been inside their building for about four hours when we came across a row of filing cabinets that must have contained some important documents. About ten tall filing cabinets stood in a row, and each of them had a vertical bar attached to the cabinet with a padlock securing the bar to the cabinet. This was more security than we normally saw on these kinds of cabinets.

When we were working on the inside of a building, we tried to look at everything we thought could be a vulnerability. I took the time to quickly examine every lock on these filing cabinets. It wasn’t surprising to me to find one that looked the same as the others on the outside, but that was drastically different on the inside. Someone had replaced one of the pin tumbler padlocks with a warded padlock. In less than ten seconds, I opened the lock, taped my business card on the INSIDE of the filing cabinet to prove we had been there, and closed the lock again. The bad guys could have accessed the entire contents of that file cabinet just as quickly.

Continued
Let’s look at a few types of locks to help you learn which ones are better than others:

Figure 1.1 shows a pin tumbler Master brand padlock. It’s the exact kind of lock we saw on most of the filing cabinets. Pin tumbler locks are also the most common type of lock we see on doors in homes and office buildings. These locks can be picked, but I’ve never been very successful with such endeavors.

**Figure 1.1 A Pin Tumbler Master Brand Padlock**

Why was this one lock different from the rest? I suspect that someone either lost the key to the original (more secure) lock, or lost the lock itself. If that happened, they could have simple gone to the hardware section of their local store and purchased a lock that looked like the rest of the locks on those file cabinets. If they went with the mindset of most people that I watched purchase locks, they would have purchased the least expensive lock they could get, as long as it looked as strong as the original lock.

The warded padlock (shown in Figure 1.2) that we found on one of the filing cabinets looked about the same, but it had a different keyway.
I was able to open this one in less than 10 seconds, and you could, too. Opening locks like this isn’t even lock picking in my opinion. The pick sets for these are more like master keys.

In Figure 1.3, the key on the left is the key to the pin tumbler lock. The one on the right is to the warded lock. This is really basic information for anyone familiar with locks. My experience has been that most people aren’t even a little familiar with what makes a lock reasonably secure (or very insecure). If they were, they wouldn’t be out there buying the cheapest locks they could find as long as it looks strong.
So, are there any padlocks that are reasonably secure and not terribly expensive? My favorite has always been a lock that looks a little different, but has a lot of leave-me-alone features (see Figure 1.4). This lock, the Abus Diskus No. 24, is made in Germany and is quite secure for its $25 price tag. It’s a pin tumbler lock with all five of its pins being mushroom-type bottom pins. There are people out there who can pick it, but I’ve never successfully picked a lock with any mushroom pins, much less one with all five pins being mushroom pins.
If we want to talk about the grand-daddy of all high security padlocks (in my humble opinion, and I’m not alone), we need to take a look at a lock that has been at the top of the list for several decades. My winner here would be my favorite (I have five of them myself) combination lock, the Sargent & Greenleaf 8077AD. It’s a 1.5-pound fortress in so many ways. From the outside, it doesn’t look all that impressive, but it is! Just enter the name S&G 8077 in Google, and countless articles will pop up about their strength and reliability. Just like anything else in life, you get what you pay for. These are not your $5 combination locks, however. The non-government model is still available in many places on the Internet, at prices ranging from $165 to $325 (or more). I do see them frequently on eBay at great prices and they’re worth every penny. Figure 1.5 shows one of mine.
Now, let’s talk about due diligence a minute. This was something I explained to all the groups that hired us to perform penetration tests during our exit interviews. Regarding locks, there’s no way to keep a determined and knowledgeable “bad guy” from getting past whatever security measures you place in their way. Even the best burglar-resistant safes are rated according to how many minutes it would take an educated thief to open it. Your task is to show you did whatever you could to make it as difficult as possible for someone to get to your valuables. A simple example of improved due diligence would be to replace the locks (even the pin tumbler locks) on most of the filing cabinets in the earlier war story, with locks like the Abus, or the S&G 8077 combination lock. The difference in cost for the entire row of ten filing cabinets would be less than $200 TOTAL for the Abus locks and about $3,500 max for the S&G locks. These locks will be protecting some pretty important stuff, so isn’t
it worth an extra $200 to $3,500 to gain some considerable security while at the same
time increasing your due diligence efforts? I don’t think for a second that an additional
$200 (or even $3,500) would make a difference as far as expense goes. Most of the
firms I was involved with during these penetration tests wished to prevent millions of
dollars in possible espionage losses. They simply didn’t know that this small change
could make such a big difference for their company. It may have prevented the event
that had us in there in the first place. That’s why books like this one are so valuable.
One or two “techno-tidbits” as I like to call them can make a huge difference in your
overall security posture. While this book is titled *Techno Security’s Guide to SCADA
Security*, in my mind, its real value is in explaining how to prevent a lot of bad things
from happening to anything that is important to you even if it doesn’t impact our
nation’s critical infrastructure.

**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 of the store with your brand new one. I’m not
suggesting that you don’t buy a new (soon-to-be-old) computer, you just need to
realize that you’re going to most likely need a new one in about two years.

What happens when that “elephant” you purchased a few years back 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
our vulnerability tests from 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 1.6 offers some examples I found on the Internet, showing a set of picks very similar to the set I’ve owned the last 30 years. LockPickShop.com is the company where we buy our locksmith supplies for our training classes. Their outstanding response and customer service, and their quality products, have kept us coming back for years. Figure 1.7 shows a pick gun that’s also similar to mine. Pick guns don’t take a lot of practice to learn how to use. If you are thinking about running out and buying some of these tools, please be sure to read the warning I have included with 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 1.6 The LockPickShop.com Web Site**
Once we found a room that obviously contained some outdated equipment, we 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 cases.
back up. How valuable was the information on that drive, and how soon would you know that the drive itself was now missing from the elephant burial ground?

Most likely, you will never know that 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 some 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. It’s likely the crime could go completely undetected.

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 I just described, of which I didn’t go into detail here. Nevertheless, here’s the bottom line from my experience with these old drives: If they weren’t properly wiped clean, and if the drive itself was operational, we were able to get to the data on them without any 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 to own a drive this size for a mere $1 per megabyte. Now, I’m seeing 200GB disk drives on sale for around $50 (after rebates). That’s about 25 cents per gigabyte, which means that the same $1 per megabyte I paid (actually worth less today) would buy me 4 gigabytes or 4,000 times as much storage space for the same dollar spent.

The advice here is to be careful with those old disk drives. This applies to the computers at home as well as at the office. There is much valuable data on them, and the risk grows as the storage capacity of every drive rapidly climbs each year. Let me share some of the most effective tools I have seen for really being sure that your valuable proprietary information is gone when you dispose of a broken or outdated hard drive.
The first of these is a device called Digital Shredder sold by DestructData (www.DestructData.com), which insures that your valuable information is gone from the drive before it is reused or destroyed (Figure 1.8). Once Digital Shredder has done its job, the disks can be reused (knowing for sure that all data has been removed) or they can be completely destroyed using a device that I found most interesting for complete drive destruction.

Figure 1.8 Digital Shredder from DestructData

The second device will render the drive completely unusable by punching a large hole thru the middle of it. Figures 1.9 and 1.10 show a destroyed disk drive and the machine that destroyed it. And here’s the URL to the Web site of the only company I’m aware of that offers the complete destruction of obsolete hard drives: www.edrsolutions.com.
Figure 1.9 A Destroyed Disk Drive
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 a very small percentage of “dumpster divers” ever get caught. As simple as this problem seems, it isn’t one that is 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 to look through your own dumpster occasionally. (I highly encourage you to do just that.) There may be old company phone 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 listed on them, and so on, and so on.

It doesn’t take much imagination to think of all the potential problems that could have their beginnings right there in your trashcan. Someone who is trying to pretend 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 the “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 place.

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 and employee awareness of the problem will help correct it. The 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 confetti instead of long strips. I guess it’s theoretically possible to reassemble a crosscut shredded document, but if it falls into a bin with a large number of other crosscut shredded 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 about what they said and what they threw away. (I wasn’t around during World War II, but I was the product of a happy home after the war.) As individuals and companies, we need to bring back just a little bit of that 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 stays in our trashcan that clearly 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 little thing I can do to protect my family from things like identity theft and credit card fraud helps me sleep at night.

**Employee Badges**

I know employee badges 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 that we belonged there. Not only were we inside their buildings, but we were also inside 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...
it was fake. During one of our security meetings, I told everyone in our group about my little experiment and most were quite surprised it was never detected.

Part two of my experiment offered the most interesting results to me. I created a picture showing my two IDs side by side. The fake one was quite obvious when seen next to the real article. We began to teach people how to take a slightly closer look at the IDs people 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 the number of my friends, who after a training session, spotted the fake ID as I passed them in the hall. Some would see it from ten feet away. These were the same people who, before the training, hadn’t even noticed it while sitting three feet from me in my office. 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” to ask for identification.

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 employing biometrics scanners and other high-tech devices. As with everything else in the security field, you need a system that is appropriate in cost to 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 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 very 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 crosscut shredder.

Tip

If you have too much invested in your strip cut shredders to replace them, at least consider purchasing some of the small crosscut shredders and place them directly in the offices of people who have especially sensitive documents that should be destroyed. These small crosscut 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. Once you start doing this, it will become second nature and you’ll never have to worry about anyone seeing your personal information once it leaves your home. Especially since 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 during 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 that are too bulky for my shredder. It’s a great way to clean out the barbeque 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 conducting a test, the first thing we went for were corporate and agency phonebooks. Once we got our hands on a corporate directory, the social engineering began. Most corporate phone books 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 were challenged further. 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, filing 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 (we might even get hit if you throw them in while we’re there looking for goodies).

If paper directories can be eliminated altogether, that would 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 since 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 note on the side with the person’s login ID and password scribbled on it. Once we logged onto 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 sticky notes with login IDs and passwords. Maybe this 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 that 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 use at least some form of two-part authentication that employs either biometrics or a handheld authenticating device of some type to attain two-part authentication. Fortunately, some forms of biometric access control are becoming very reasonable in price. So, everything you do in the way of authentication will greatly reduce your vulnerability to this form of instant identity theft.

Tailgating

Tailgating was one of our most successful entry techniques, regardless of a building’s security procedures. For some reason, people in the outside smoking areas never questioned our being there or walking in behind them as they returned to work. We found that many corporations had good security at their main entrance points, but were lacking at other entry and exit points, allowing us 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 them as we pretended to search for our imaginary access cards.

**Tip**

Here again, companywide awareness training and a strong security policy can go a long way in preventing this type of entry. These outside break, lunch, and smoking areas are frequently places where there are no security guards or receptionists 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.
Warning

The countermeasures for this vulnerability really aren’t as simple as we might think. Most employees who enter a building aren’t security people. They are simply trying to return to work. Even though someone trying to enter 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 should be trained on when and how to notify security if they suspect an unauthorized person has followed them in.

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 thru 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 if 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 having an effective bomb incident plan are another countermeasure that can be employed with considerable effect.
Case Study

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 in the Chicago area asking for help. He said his company had office locations in several cities throughout the country and one office outside it. A series of bomb threats called into their corporate headquarters was causing them to lose a little sleep. They just wanted our team’s suggestions about what they should do. This meant a trip to Chicago for us in February. (Being the warm-blooded person from the sunny South that I am, this was a bit like 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 anything out about his company. It could also provide a possible 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 that their corporate attorneys and risk managers attend the training as well. They were going to learn everything they wanted to know but were afraid to ask about bombs and bomb threats.

We arrived a day early, and we 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 could allow someone to easily place a bomb in or just outside their building. The outside 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.

When I stated that a simple metal coat hanger might be able to compromise the entire system, my fellow team member gave me a strange, “you’ve done it now” kind of look. 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 that had hired us was standing 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 that I had been asked to break in through, it was still like Iceland in February. I politely said that I would go outside (without my coat!) and try for a few minutes to gain entry. All that I asked was that if I started to turn blue, to please please please “open the door from the inside and let me back in.”

In the end, it was an unnecessary request. I was back inside in less than 30 seconds as everyone looked on with that patented deer-in-the-headlights look, after I’d calmly breached a quarter-of-a-million-dollar security system with no indication that I’d ever touched it. This was not the first time I’d seen this issue with an improperly adjusted access control system. The system was one that, detecting motion from the inside, automatically unlocked the door as someone approached it to exit. I had noticed that 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 briefly 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 concerning 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 consisting 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 your their probability threat and something they needed to address immediately in our opinion.
Spot-Checking 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 that 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’d 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 would may be amazed at what you find hidden up there (hopefully it’s not ticking!).

Checking for Key Stroke Readers

Some of our favorite tools are the software and newer hardware versions of 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 time frame, we would install a keystroke reader on their workstation during 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, they look like they belong there to the casual observer. The one we used looked like the induction coils we used to see on some of the older parallel printer cables. It just doesn’t look like anything you need to worry about.

If you didn’t put it there, you better worry, because it’s logging every single keystroke you type in!

The version we used could hold about 500,000 characters or a half a megabyte. That might not sound like much, until you consider that the Word document that eventually became this entire chapter took up only about 20,000 characters (16,000 characters for the text and about 4,000 backspace key strokes to correct all 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 nonprinting character entered as part of a password or whatever. It only records keystrokes, so it holds a lot more information than you might think. We have left them connected to target computers for up to three weeks and still the user’s activity only filled up 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, meaning everything will be in the clear when someone (hopefully only you) looks at the data that 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 that lives behind most computers and see if anything looks strange. Unless you have been made aware of what they look like, it probably won’t look strange to you even if you do see one. I pass one around for people to see at every one of my security training classes. Statistically, I’ve read that people are 27 times more likely to remember something if they can see and touch it. I usually ask my attendees for a show of hands by those who have 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. Figure 1.11 shows the workstation in a minimum configuration 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 into 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 of these on cables found behind most workstations.

**Figure 1.11 The Back of a Normal Workstation**

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 1.12). 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 we 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 that the computer would know it’s there. It uses virtually no power, and doesn’t require any software to be installed to make it work. When I finally remove it and take it back to check out the internal log, the computer (and you) would never know it was gone again.

This device can be used as an excellent security instrument if you suspect someone is using your computer when you are not there. It is sold primarily for that purpose. This is a good thing, as long as you know it’s there.

Checking Those Phone Closets

If your building is in a rented space, or in a multi-tenant building, it’s a good idea to have someone perform a thorough check of your hard wiring for the phone lines. You don’t know who was in there before you were, and old wiring is sometimes not 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. This is the 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 right near the modem. We found many PBXs that we “visited” in the evenings to be very social-engineer friendly.

Removing a Few Door Signs

It always amazes us to see rooms that have a sign over them saying Computer Room or Phone Closet. Obviously, the people who work there know where it is, and there’s no reason for anyone else to know what’s inside. It’s all right for the room to have a number on the door that building maintenance would understand, but there’s 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 re-enter the building and try to be seen by the building security cameras that 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 eventually report us. As far as we know, we were never reported as being seen on the tapes recorded by those cameras, so 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 simply 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 entire expensive surveillance
system is worthless if whatever is captured on tape isn’t ever seen by a human who can do something about it.

This is another area where I believe that the people responsible for the techno security of the systems need to talk to the people responsible for physical security. Cameras and lights have always been countermeasures that I like to see in and around buildings and personal homes. They can scream “Go find an easier target!” to the bad guys of the world. There may be areas where additional cameras could be recommended to help improve the security of critical areas or rooms. The team responsible for overall physical security might not know about these areas unless you tell them. They may already be monitoring areas you aren’t aware of, which could help you if you have an incident.

The reason I mentioned personal homes several times throughout this chapter is that this can be another area of vulnerability for physical penetrations or social engineering attempts to gain specific information. Many people now do much of their work from home on workstations connected to the Internet at high speed. I employ as much physical security at my home office as I have at every other office where I’ve 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 very safe knowing that it would be difficult to attempt anything around our home without someone knowing about it. The security cameras are also motion-activated, so the only thing I see is recorded activity where movement was 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 in their buildings. These are not the same kinds of light controls that I installed around my home. Those would help on the outside of any building. What I am talking about here are the motion sensors that turn on the lights inside an office or room when someone walks in. These same sensors turn the lights off after a pre-set time once the final person leaves the room.
Every penetration test that we were hired to conduct had several buildings of opportunity for us to attempt to enter, and every one of them had at least a few lights on all night long. While we were conducting our initial surveillance of the buildings, that was one of the first things that we noted. Are there lights left on at night, and if so, were they the same lights every night. In most cases, with a building having about 15 floors, there would be six or eight lights 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 created a good situation for us. If a random number of lights were left on each night, the security forces would not have any easy way to decide if everything was “normal” at any given time.

As they patrolled from the outside (we were watching them do this from the outside and from the inside once we got into the building), they really had no reference for what would be 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 there was no human around needing light could eventually pay for the additional cost of the sensor.

**Let’s Go to Lunch**

This little problem remains high on my list of things we should all be considering every time we go out for a meal in a public place. Many of our office buildings have public restaurants either in the building itself, or close-by within walking distance. Here’s what I think happens all too often. We’re at work discussing something important, and someone realizes that it’s time for lunch. Out we go to the local fast-food restaurant of choice that day. There’s no reason to let lunch slow down our train-of-thought for the project we’re working on. The in-depth conversation about that new marketing scheme or the great new product we’re about to announce continues as if we were still back at the office.

You would be shocked at how many of these kinds of conversations I’ve heard over the years in public places. Things were discussed in the open, among total strangers,
that should never have left the corporate boardroom. It just seems like we are all too busy to stop and think about security, and controlling who has access to our proprietary information. I occasionally get a chuckle from my friends when I remind them of a time when the national security message was “loose lips sink ships.” (That was during World War II, which was just a little before my time, and I do mean just before.) Judging by the conversations I have had with some of the people who were alive during that time, pretty much everybody took security seriously. Why has that changed so drastically in our high-tech world just 60 years later? We certainly don’t have less at risk than they did then. If anything, we have much more at risk, especially in the world of technology. People were careful and concerned that there could be spies anywhere. Has that threat gone away? I don’t think so.

There couldn’t be a better example of No Tech Hacking than simply sitting in a crowded restaurant on a typical day, in a typical city, and listening. The technology that exists today for helping people hear things a little better didn’t even exist in the “loose lips sink ships” days. These are legitimate devices that can help anyone with a hearing problem hear MUCH better. I’m not talking about hearing aids; I’m talking about amplified listening devices that are available just about anywhere. A couple of them are shown in Figures 1.13 and 1.14.

Figure 1.13 An Amplified Listening Device
This is the smallest sound amplification device that I found at my local Radio Shack. This picture was taken with the device sitting on the anvil (back) portion of my portable vice. I’ve left a key in the device (visible at the bottom of the picture) to give you a reference as to the size of the device. It’s pretty small. The sound amplification is amazing considering that this device only costs around $10. Let’s take a look at a higher-end version of the same component.

**Figure 1.14 A RadioShack Amplified Listener**

The one in Figure 1.14 is a little more expensive and uses a single AAA battery that is easily replaced. The quality seemed to be about the same as the smaller, less expensive model. It cost about $25. With so many people today using MP3 players and other small devices with earphones, you need to be aware that these devices might not be noticed in a crowded public or private meeting space. My purpose in describing these kinds of devices is to make you aware of how available they have become at a very low cost. They have plenty of valuable and legal uses. You just need to be aware that some people could use them for other purposes. Have a nice lunch....
Fun in Manholes

This is certainly not a new topic, but it is one that I suspect most people don’t ever think about. Those of us who work in major cities, and even in small cities, walk over manholes every day. That’s certainly nothing to be concerned about, but do we ever consider what’s under those small circles of metal? While most companies don’t own the manhole covers (and what’s under them) surrounding your building, it’s still a good idea to check on their security. The extent of the infrastructure that exists below the streets of most cities is incredible. Figure 1.15 a boring picture of a boring manhole on a boring street. Pretty neat, huh?

Figure 1.15 A Boring Manhole Cover

Things get more interesting when we take a brief look at what’s under some of them (see Figure 1.16).
Figure 1.16 A Ladder to Trouble
Figure 1.16 shows a ladder on the underside of a manhole and it’s about 10 feet long from top to bottom. I wouldn’t want to fall into that one if someone removed the cover on a dark quiet night. If you enter the words “manhole security” in Google, you’ll find a few interesting articles about how manholes can now be protected, as well as a few stories that discuss the problem in some cities with manhole cover theft.

One of my fondest memories of a manhole in the movies was seeing Mother (Dan Aykroyd) working away in a nearby manhole at the beginning of the movie *Sneakers* in 1992. His penetration team was hired to test the security of a bank. The story was pure fiction, but the vulnerability of what could be accessed from within certain manholes was real. Figure 1.17 shows a manhole cable vault that Mother would have been proud to work in. This picture was taken from the base of the ladder shown in Figure 1.16.

**Figure 1.17 A Manhole Cable Vault**
Most manholes like this have long since been secured, especially since 9/11. That doesn’t mean you shouldn’t become aware of any manhole that could be used to access your building. This is even truer for multi-tenant (that’s most of them) buildings in large cities.

Internal Auditors Are Your Friends

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 for improvements in a certain area. Many of the larger corporations have information system auditors, who have the primary responsibility of looking after the technical world within a corporation. That’s a lot to keep up with.

Most mid-sized corporations have internal auditors who are responsible for IS in addition to their usual audit tasks.

Always Be Slightly Suspicious

The number one countermeasure for the threat of social engineering is to be just a little more suspicious than we normally are as good friendly trusting Americans. This holds true for social engineering attempts that come by way of a phone call, or a visit from a friendly salesman. The same principle will help all of us be more aware of possible terrorist planning activities as well. We all need to be just a little bit more aware of what is going on around us and who is possibly trying to pretend to be other than who they really are as they use that age-old skill of social engineering to try and breach our security.

Unfortunately, this is a difficult countermeasure to continue to implement. We simply just stop being concerned about things that happened only a few years ago. I suspect this has something to do with our wonderful freedom from most of the things that people live with every day in other parts of the world. We can never afford to become complacent again. If we do, it will make life much easier for future bad guys, social engineers, and even terrorists. This and most of the countermeasures suggested in this chapter help to mitigate all of these threats.
Getting 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 overall protection process. I know that I’m not the only one who has ever mentioned this.
Summary

I’ve thrown a lot at you in this combination of risks, threats, vulnerabilities, and countermeasures associated with SCADA security concerns. What I have tried to address in this extended chapter are what I consider the low-hanging fruit that the bad guys of the world 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 even be responsible for correcting many of the vulnerabilities, but you might be able to get this book to someone in your organization that can correct them.

Security will always be a long-term team effort. This is true for every size company as well as every size family at 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 are in a very technical world that will do nothing but get technically more complex, we should never forget about physical security at home and at 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.

Solutions Fast Track

How Easy Is Social Engineering?

- Social Engineering is something that anyone could easily fall victim to.
- Knowledge of the threat and employee awareness are the major countermeasures.
- Unfortunately, it is still way too easy to con someone out of proprietary information regarding physical access.

Human Nature—Human Weakness

- The threat of social engineering is a risk management issue.
- Most people are way too trusting of friendly strangers.
- Always be just a little bit suspicious until you know for sure whom you are interacting with in person, or on the phone.
Physical Security and Social Engineering Countermeasures

- Employee awareness training explaining social engineering and how to become a less likely victim.
- Role play (it can be fun) to show examples of social engineering.
- Conduct little internal social engineering tiger team attacks and share the lessons learned (or not learned the first time through) with employees.

Dumpster Diving Still Works

- It’s amazing what we still find in dumpsters. Much of it should have been shredded.
- Crosscut shredders are now very inexpensive and effective at home and at work.
- Consider crosscut shredders at every desk where important papers could accidentally be thrown in the trash.
- Shred EVERYTHING that comes into your home with anyone’s name on it. You don’t need to shred the entire document or magazine, just the pages where a name or address appears.

Beware of Tailgating

- Most of us kindly hold the door open for someone walking in behind us.
- Security policies should be clear as to what employees should do if they suspect that someone who doesn’t belong in the company has followed them into their building.
- Avoid potential workplace violence incidents by following your security policy.

Check for Keystroke Readers

- Hardware keystroke readers are very hard to detect.
- News reports indicate that these are now being found in public access workstations.
- This threat is another employee awareness issue to be covered with all employees.
Check All Locks for Proper Operation

☑ Check all locks at home and at work. Report malfunctioning locks.
☑ Don’t prop doors open and report any that you find propped open.
☑ Change the lock combinations (have them re-keyed) when you move into a new or used home. You never know who has that extra key.

Let’s Go to Lunch

☑ Be extra careful what you talk about in a public restaurant.
☑ Be aware of the people around you or sitting close by.
☑ Also be careful what you talk about on elevators. You never know who is listening and why.

Fun in Manholes

☑ Be sure that someone in your company knows just what’s under your building.
☑ If you spot a potential building entry point, report it to your security group.
☑ Every major city has a considerable infrastructure underground with access through manholes.
Frequently Asked Questions (and Special Interviews)

Writing chapters in books isn’t easy. This is the fifth book in the Syngress/Elsevier library that I have had a hand in the past 18 months. Even writing a single chapter is really time-consuming hard work. Many internationally known experts are long-time personal friends and acquaintances of ours, and most of them have a lot of experience to share with us on some critical subjects. Unfortunately, most don’t have the time available to write a complete chapter in one of our books, but I still wanted them to share something with us. The solution to this dilemma was to include some of their knowledge as a special section in this opening chapter, substituting (in a way) for our books’ usual end section of frequently asked questions. Here, I will conduct a series of interviews, and ask the questions, prodding the experts about their respective areas of skill. So, let’s dive into the interviews!

Critical Infrastructure
Emergency Communications

Special Interview with Phil Drake,
Telecommunications Manager, The Charlotte Observer, Charlotte, North Carolina

Jack: The ability to continue to communicate is certainly critical to keeping our entire critical infrastructure secure. Share with us some of your thoughts on ways to continue to communicate in emergency situations.

Phil: The first step is to have a plan to be able to communicate in any situation. Having the most modern equipment and the best responders are of no value unless you can deploy them when and where needed. If you can’t communicate with your assets, you are part of the problem, not part of the solution. Have an emergency communication plan, test it routinely, and be certain that everyone understands it.

Jack: If a department or agency does not have a plan specifically addressing what to do when their communications links fail, where do they begin the planning process?

Phil: Plan to communicate under any circumstances. Approach planning with a “what if” attitude and expect the worst. If one system fails, for whatever reason, have another system or plan ready to take its place. If the primary system fails, what’s your backup? If the backup fails, what’s next? I know of a number of agencies who have
well-designed plans and multiple layers of communications links but in testing they still can’t communicate with some of their key assets. The reason? The people in the field didn’t remember what to do or were never told. Have a plan, document it, test it, and be sure everyone understands it.

**Jack:** In emergency communications, what’s the number one concern?

**Phil:** People. That’s not the answer you expected, but it’s the most important.

Every company and government agency must ensure that its people (work force) have the necessary plans, training, and equipment so they can respond to an emergency when needed. This includes the day-to-day “onsite emergencies” and it’s especially true for a natural disaster or other event that affects the employee’s home life. A major part of this readiness is personal and family disaster preparedness. If an employee’s family is safe, he or she will return to work much quicker and can focus on their job. My employers feel that this level of preparedness is not their concern; it’s a serious mistake.

Following workforce preparedness, electrical power is the major concern and dependency. Commercial electrical power may be unavailable for days or possibly longer periods following a disaster. We have some of the greatest communications technology imaginable, but it still is totally dependent on “old fashioned” electricity. You’ve got to power your equipment, and whatever communications infrastructure you depend on must have power to support your communications needs. The majority of large agencies and businesses have backup generators powering uninterruptible power supplies (UPSs) for fixed and wireless communications equipment. Smaller businesses tend to avoid the expense of this protection and “take their chances.” It’s important to understand the impact of a power outage on the operation and its ability to continue to provide the products and/or services that are expected.

The majority of cellular carriers provide backup power at many (but not all) cell sites. Public safety and most business radio systems have emergency power. Our dependency on wireless keeps growing, so talk with your service providers about their backup power plans. Here are a few questions to ask:

- Is the entire system protected by backup power?
- Will the system “footprint” or coverage area be decreased in a power outage?
- Is the emergency power provided by a generator, batteries only, or a UPS (uninterruptible power supply)?
- What’s the “run time” on emergency power before the batteries need recharging or the generator needs refueling?
While operating on emergency power, will the system support normal traffic levels? (In an emergency, communications systems will carry more traffic than during normal conditions.)

Backup power is so important that the FCC has mandated that every telephone central office, commercial two-way radio system provider, and cell site have eight hours of backup power by early 2009. The “land line” phone companies have operated on battery power backup up with generators since the start of the industry. That’s not the case for the wireless or land mobile industry. There are over 210,000 cell sites in the U.S., plus all those other operations just mentioned. So while it’s a great idea, it’s not going to happen anytime soon. The cost, space requirements for battery banks and generators, plus the wireless industry attorneys will slow the implementation down to something more realistic.

Now let’s switch to the “end users”—the responders or field personnel depending on the communications system to save lives and/or serve their customers. In a protracted emergency, can the users charge their handheld radios and cellular phones without commercial power? Is a supply of alkaline (non-rechargeable) batteries available for two-way radios? Does every cellular phone and laptop PC have a 12-volt cigarette lighter adaptor cable?

Twelve-volt inverters are another excellent investment that will provide emergency power from your vehicle’s battery. These small boxes plug into the cigarette lighter outlet (now called the 12-volt power outlet) and provide 110-volt AC power. They come in various sizes and technologies, so shop around and get a model that will supply your needs. Large inverters connect directly to the vehicles’ battery, smaller ones plug into the 12-volt outlet. A decent one will power a laptop, a TV, or charge radio and cellular batteries.

Other 12-volt or low voltage D.C. solutions include an increasing number of products hitting the market with “hand crank” power supplies. A minute or two of cranking supplies enough power to operate an AM/FM radio, lantern, or even charge cellular batteries.

Small inverter generators are also an option. These generators produce DC voltage first, and then convert it to 110 volts AC. The conversion process produces very clean voltage that is well suited for communications and computer use. These tend to be more expensive than the normal gasoline-powered generator, but are worth the extra cost. Buying a brand name will provide a much quieter generator and that’s an important consideration in any communications operation. While power may be our
number-one communications concern, safety is always our ultimate concern when operating any mechanical or electrical equipment. Read and follow all instructions. Gasoline is dangerous in normal conditions, and especially so when conditions aren’t normal. So be careful.

**Jack:** You’ve used solar power in the past to power some of your emergency equipment. Are you still doing that?

**Phil:** Absolutely. The technology has advanced dramatically in the past few years. We now have fold-up solar panels that can charge and power radios and satellite phones. These panels are formed onto high-density flexible material that’s very tough and waterproof. A 25-watt, 1.5-amp panel measuring $8 \times 11 \times 1.5$ inches unfolds to a little less than $2 \times 4$ feet and weighs less than a pound. Currently, they are a bit pricey but worth the money as they are non-polluting and very compact and totally quiet.

**Jack:** You once told me that you used two telephone companies for critical locations. Why?

**Phil:** Using two “local telephone companies,” the incumbent telephone company (for example, a Bell company) and a “CLEC” or “competitive local exchange carrier” eliminates a single point of failure and allows you to take advantage of some new creative pricing arrangements offered by the competitive companies.

This is not a complicated process. Your company or agency can simply use one phone company for outbound calls and another company for inbound calls. You may want to split your range of telephone numbers and let one company provide inbound services on half of the numbers and another carrier to carry the other half. Lowering the costs of communications and doubling the diversity will make everyone happy.

You may ask: Why bother? Well, we live in interesting times and the communications infrastructure is a target of those who would do us harm. The big telephone companies are big targets in this new arena of terrorism. They take extraordinary steps to protect their facilities and services. Your workplace or agency should take protective steps too, to improve your chances of surviving a service interruption.

**Jack:** I know you used satellite links extensively during Hurricane Katrina. What’s new in that technology?

**Phil:** Portable/mobile satellite phones and service are almost common now for any organization tasked with disaster communications. Hurricane Katrina certainly proved the value of satellite service for any company or agency that was there and had to stay operational. Mobile, stationary, and handheld units have dropped in size and price. One newer entry is BGAN (Broadband Global Access Network), which is
IP-based and allows users to connect to the Internet and conduct voice calls simultaneously. These units are also available in small (about the size of a laptop computer) and smaller (about half the size of a laptop). Higher bandwidth is available and comes with larger antennas, power requirements, radio equipment, and, of course, larger prices.

Satellite links for SCADA installations are becoming much more common and affordable. Security of the data, higher link speeds, and reliability are major justifications for considering replacing traditional communications links with satellite where appropriate.

"Ham" radio operators have a saying: "When all else fails, amateur radio works." I have yet to find an EOC (Emergency Operations Center) that does not have an amateur radio station onsite or access to one nearby. Emergency management agencies, the American Red Cross, and the Salvation Army partner with amateur radio clubs to ensure reliable communications when disaster strikes. The private sector too can benefit from knowing which of their employees have "ham" licenses as they can provide emergency communications to provide health and welfare reports between employees and their families when the need arises. A private sector enterprise, for example, may provide products and services that would help the recovery process in a disaster. Having trained radio operators capable of communicating with emergency management officials will benefit the enterprise and the community.

There are a number of organizations within the ranks of amateur radio that train ham operators in emergency operations and traffic handling. These skilled volunteers spend many hours training in sometimes-primitive conditions to duplicate disaster situations.

Annual "Field Day" exercises allow "ham" operators to test their emergency skills under simulated disaster conditions. It's also a great opportunity for the public to see first-hand what critical services this "hobby" provides. These unpaid volunteers have a long history of providing critical communications when the need arises.

**Jack:** Most offices have a centralized telephone system. Are there any "preparedness points" for companies or agencies to check?

**Phil:** Is the system protected by a UPS and is the UPS backed up by a generator? If so, is the generator routinely tested and serviced? Are the UPS batteries replaced when recommended by the manufacturer?

As mentioned earlier, having carrier and central office (where your local communications circuits originate) diversity is very important. If one carrier or central office suffers an outage, the other will most likely be unaffected.
If the phone system (PBX for Private Branch Exchange) stops working for whatever reason, is there a plan in place to provide communications in the most critical areas? Most phone systems are installed with a “power fail transfer” switch. This small device senses if power to the PBX and related equipment fails and then bypasses the affected equipment by using a limited number of “outside” lines. These lines are automatically connected (on a one-for-one basis) to extensions (telephones, fax machines, or modems) in the facility. These extensions should be marked as “emergency phones” and their use explained.

Another preparedness method is to have a number of outside lines ready for use that can be manually switched to nonfunctioning extensions in a PBX failure. A two-position toggle switch can be used to switch the extension between the PBX for normal operation, and the outside lines during a service interruption.

If your “PBX” is now a server in a VoIP (Voice over Internet Protocol) installation, there are additional concerns if the LAN (local area network) fails. In these systems, the voice communications are carried over the LAN, not telephone wiring as in the traditional PBX system. Most system designers and vendors provide a number of “failsafe” phones (these are generally analog or “POTS” telephone sets) that are hard-wired the old-fashioned way to protect them from a network failure. Again, it is important to clearly mark these extensions and [make sure] everyone knows their locations.

**Jack:** Is cellular an infrastructure or “tool” that you recommend for emergency use?

**Phil:** Yes, but with some reservations. Public safety and service operations, industry, and the general population so depend on cellular technology today that during an emergency, there simply isn’t enough cellular capacity to go around. Businesses particularly need to keep this in mind if their “emergency communications plans” depend entirely on cellular phones—which many do unfortunately.

When we mention cellular, we immediately think of the standard flip phone, but one very good cellular “tool” to consider is fixed cellular. These special cellular devices are excellent backup for critical landlines that might experience an interruption in service, or for use in a remote location where phone service for alarms or monitoring are unavailable. These cellular transceivers operate on 110-volt power and use an antenna, which is usually mounted outside the facility. These units have the ability to sense a telephone line failure and automatically provide a cellular “dial tone” to the telephone set or other device until service is restored.
Public safety and government, who are huge cellular users, faced the same problem of “system overload” during emergencies and needed a solution. Enter the National Communications Service (a federal government agency) and their WPS (Wireless Prioritization Service). This service allows certain key leaders (local, state, and federal) plus others who are authorized, to have cellular access at a higher priority than general users. A W.P.S. user will be able to make and receive calls while others will get fast busy signals. Anyone with key leadership or emergency response duties should investigate this service.

Cellular providers not only provide cellular telephone and “walkie-talkie” voice services, they have some very robust data services that anyone who needs to stay connected should investigate. This cellular-based Internet access is generally delivered via a PCMCIA card, “ExpressCard,” or a USB modem. Simply plug the card or modem into your laptop, or if it’s built in, just click on the icon, and in less than a minute, you have broadband Internet access almost anywhere. In an emergency when voice channels are overloaded, the data services continue to carry traffic at near normal levels. This is due in large measure to engineering and the fact that there are still more voice users competing for finite resources.

BlackBerries and other PDAs are the largest users of cellular data services. These devices provide access to e-mail, the Internet, and a host of applications that make the mobile user very productive regardless of location. In addition to the traditional communications methods (e-mail, voice, and text messaging), BlackBerries have the ability to text message unit to unit, bypassing the organization’s exchange server, BlackBerry Enterprise Server, or the Internet, which may be inoperable during disasters or other more localized emergencies. Using only the unit PIN (personal identification number—each BlackBerry device has its own) and the cellular data network, this BlackBerry-to-BlackBerry communication can provide a critical link to key personnel during a crisis.

Jack: You just mentioned WPS, which is a federal program to help communications keep flowing during an emergency. Are there other programs that may help our readers?

Phil: Here are two others that may be considered:

GETS (Government Emergency Telephone System). This telephone communications network is managed by the NCS (National Communications System) and is a workaround for a congested or damaged public switched network. Government employees, emergency responders, and certain private sector businesses can qualify for GETS. Users are issued access cards, which contain an access telephone number and a
personal identification number. Dialing the access number and entering the PIN allows the user to place a telephone call over a highly protected telephone network.

TSP (Telecommunications Service Prioritization) is a registration system for listing critical telephone and other communications circuits. In a disaster or other emergency situation, these registered agencies or companies will receive priority repair and restoration service from the local telephone companies and long distance carriers. Any company, agency, or organization that provides critical support for the public or government will probably qualify. This program also falls under the National Communications System.

One of the most reliable and cost-effective communications methods for emergencies or any other time is conventional or trunked two-way radio. A private radio system or simply a number of two-way radios on commercial frequencies provides a quick and simple method of directing resources. If a private system is financially out of reach, there are numerous radio system providers in most metropolitan areas who provide the system infrastructure and radio equipment for a monthly fee.

Trunked radio systems are multi-frequency computer-controlled radio networks that provide voice, data, and telephone service to hundreds or thousands of radio units on a single system. These systems use “repeaters” (receiver/transmitter radios) mounted on high towers, buildings, or mountains that receive a radio signal and retransmit it automatically. This allows a low power radio signal to travel many miles. The majority of public service agencies around the world use this technology. “Trunking” allows the creation of virtual channels so that one group of users cannot hear or interfere with other system users even though they share the same frequencies and may be talking at the same time.

Conventional (radio-to-radio communications without computer control) radio users share the same channel or frequency even if using “select tones” or other techniques that afford users the ability to silence the radio when the information does not directly affect them. Any users can bypass the select tone and listen to all conversations much like a conference call. Conventional radio systems may also use “repeaters” to extend the range of coverage, but many do not.

A caution about two-way radio. Anything you say “over the air” can be heard by someone else. Thousands of “short-wave listeners” monitor scanners—short-wave radios—that can receive any radio frequency. Government and some public safety systems use digital signaling, encryption, and frequency hopping technology to avoid being overheard. That technology, as you might guess, is very expensive and out of reach for the majority of radio users.
Jack: Do you have any low-tech low-cost emergency communications tips to share?

Phil: I’m glad you mentioned “low-tech” because when a major disaster or incident takes away our “high-tech” infrastructure or systems, we are forced to get back to basics. Those simple low-tech tools can help us recover. Here are some tips that I share with both public and private audiences.

S.A.M.E. Alert Radio (Specific Area Message Encoding) Having an alert radio is as important as having a smoke detector in your home or office. These radios sit quietly on a shelf until dangerous weather or other local emergencies cause officials to issue public warnings. They can be programmed for “specific” counties or even smaller geographic areas to alert when conditions warrant. These radios have battery backup so if the power is off, the radio still keeps watch. Frankly I wish there was a law that every home, office, school and public building was required to have a S.A.M.E. radio. We would all be much safer.

Pagers One and two-way alphanumeric pagers are often overlooked but are still solid communications tools in an emergency. The infrastructure supporting these devices has gained capacity as customers have moved to cellular and PCS. Pagers don’t depend on the Internet or e-mail to deliver messages unit to unit and the power is generally a single AA battery. So for low-tech low-power requirement communications, these are hard to beat.

Payphones Public pay telephones are harder to find these days, everyone has a cellular phone, and so the “payphone” industry has almost disappeared. While the (almost) bulletproof case may be larger and the inner workings more complex, these are still simple old “POTS” lines that operate on phone line power. If there are payphones in or around your facility, record their numbers and make them part of your emergency communication plan.

Over-the-Counter Radios These multi-channel FRS (Family Radio Service) radios are intended for family recreation but provide excellent communications over short distances of a quarter to half mile. Using these to stay in touch with family or neighbors in a community in an emergency situation can be very helpful. They are available in electronics, discount, and home supply stores. Most FRS radios do not use rechargeable batteries, instead using easily obtainable AA batteries.

GMRS (General Mobile Radio Service) These radios are intended for personal use, but require a license purchased from the Federal Communications Commission and are more expensive than FRS radios. However, they have higher power and are manufactured to higher-quality standards than FRS radios. A number of GMRS
radios use rechargeable batteries, which of course require electrical power to recharge. Check to see if the model you may be interested in can use AA batteries as well.

A number of commercial radios are also available “over the counter” in many electronics stores and, of course, through the Internet. These also require a license purchased from the FCC and operate on commercial frequencies with less chatter. Commercial radios generally use rechargeable batteries only, so keep some extra charged batteries on hand.

**Pre-Paid Long Distance Cards** With a prepaid LD card and a payphone, you can stay in touch with local or long distance contacts.

**Citizens Band Radio** It’s still alive and doing well—in fact, it’s better now that several million users have left CBs to truckers and some hard-core hobbyists. This license-free group of radio channels can provide mobile and base station communications over distances of roughly ten miles, but this can be increased if the mobile or base is higher than the average terrain (hill or mountain for instance).

**POTS Line (Plain Old Telephone Service) and Phone** Few things can beat the reliability of a single telephone line and a wired telephone (an old-fashioned plug-in phone set with a corded handset). Power to operate the phone is provided by the telephone company central office. Employees need to be reminded that all those cordless phones at home stop working in a power failure (some do have battery backup, but they are rare and the batteries drain quickly).

---

**Special Interview with**

**J. Michael Gibbons, Principal, Deloitte**

J. Michael (Mike) Gibbons is a Principal in the Enterprise Risk Services organization of Deloitte & Touche LLP, where he oversees security services to both commercial and government agencies nationally.

Following a 15-year career with the FBI and seven years leading security practices for another “Big 4” consulting firm and an international systems integrations company, Mike joined Deloitte in 2006. During his tenure with the FBI, he was chief of computer crime investigations and established the National Infrastructure Protection Center. He was an investigating special agent in the “Hannover Hackers” case detailed in the best-seller, *The Cuckoo’s Egg*, and was involved in the first Internet worm case in the late-1980s.

**Jack:** What is the criticality of SCADA/Industrial Control Systems (ICS) compared to other important IT systems?
Mike: Even before 9/11 the government was concerned about SCADA as the world was becoming more available. Using wireless, Internet connections, and riding other network backbones, SCADA became available for inspection, interception, and subterfuge. Not all SCADA were affected, and those that managed risk according to government standards and industry best practices kept ahead of outsiders attempting to take control of them. In some cases—for example, where wireless or remote access was introduced—there were more attacks due to this new way to access the systems. Closed-end systems were inherently secure, but they actually had to be in a proven closed-loop. Outside access was the new vulnerability, in many cases introduced without the knowledge that it introduced new vulnerabilities.

Jack: Have we seen an increase in attacks on SCADA? If so, why?

Mike: If not an increase, we have seen enough to make us worry both in the public and private sector.

Insecurity of SCADA/ICS is not a theory. Several popular recent attacks on SCADA/ICS systems demonstrate the “powder keg” state of SCADA/ICS insecurity, a few being listed next:

- In 1992, a former Chevron employee disabled its emergency alert system in 22 states, which wasn’t discovered until an emergency happened that needed alerting.

- A cyber-security breach occurred at the Salt River Project, a major water and electricity provider in Tempe, Arizona in 1994.

- In 2000, in Maroochy Shire, Queensland, Vitek Boden released millions of liters of untreated sewage using a wireless laptop, apparently taking revenge against former employers.

- In 2000, the Russian government announced that hackers succeeded in gaining control of the world’s largest natural gas pipeline network (owned by Gazprom).

- In 2002, hackers disabled PLC components during a national unrest and general workers strike, crippling the country’s main port in Venezuela.

- In 2003, cyber-attacks penetrated the Israel Energy Corporation using DoS attacks but failed to shut down the power grid.

- In Ohio, the Davis-Besse Nuclear Power Plant safety monitoring system was offline for five hours due to the slammer Worm in January 2003.
In January 2003, a Romanian pair hacked into the computers at the Amundsen–Scott South Pole Station that controlled the life support for the 50 scientists there. The attackers demanded money.

In 2003, the east coast of America experienced a blackout, while not the cause, many of the related systems were infected by the Blaster worm, causing damages of US$50 billion.

In 2005, 13 U.S. Daimler-Chrysler manufacturing plants were shut down due to multiple internet worm infections.

A malware-infected HMI system disabled the emergency stop of equipment under heavy weather conditions at an international energy company in 2005.

In 2005, ARP spoofing attacks shut down a port signaling system at a Middle East sea port.

Extremist propaganda was found together with text files containing usernames and passwords of control systems at an international petrochemical company in 2006.

Given the preceding list of recent attacks, coupled with the sensitivity of information being used for communication, it is clear that attacks on SCADA/ICS systems have grown. The personal and political motivations for the attacks vary widely. In the future, the free availability of data and the weaknesses in the SCADA/ICS infrastructure could be exploited by cyber terrorists and the damage due to such attacks could be beyond our current ability to predict.

**Jack:** How critical are interdependencies between SCADA, and are they connected?

**Mike:** In the same way that critical infrastructures are interdependent, the control systems have the same vulnerabilities. Many are not yet known, as the interconnections are exceptionally complex. The evolution of SCADA to their third generation today has continued to open attack vectors still protected by obscurity alone.

The data that flows on a third-generation (WAN-based) SCADA/ICS network includes sensitive information not limited to:

- Data from remote field devices
- Activity data
- Financial data
- Real-time monitoring data
- Access control data
- Logs of access (logical and physical)
- Backup data
- Report data for various regulatory compliance
- Data used in business projections
- Human resource data
- Configuration data
- Equipment maintenance data
- Archived data (real-time data is archived)
- Historical data
- Graphs and pie charts
- User manuals

The combination of complex systems, sensitive data, and known vulnerabilities cry out for scientific exploit. Only by establishing a broad framework of protection and controls can the controls themselves be safe.

Special Interview with Kevin Manson, the Original Cyber Cop, Extranet Secure Portal

**Jack**: The ability to share information over the Internet securely is always a hot topic. Tell us a little about the robust security afforded by the Cyber-Cop portal. And is it just for cybercops?

**Kevin**: First, a bit of context or background. I have long considered myself an online community builder or “architect.” When the Internet was little more than a text medium (BB – Before Browsers), I was running a BBS on my personal computer for the Treasury Department (Federal Law Enforcement Training Center), which was connected to my home phone line, and I was “tossing” mail off USENET. This was what came to be known as the Cybercop BBS. The term “cybercop” is one which I coined in the late 80s. The mission of the Cybercop BBS was to create an online community where law enforcement could share primarily open-source information
without regard to traditional “stove pipes” or jurisdictional boundaries that had long hampered information sharing in law enforcement.

Law enforcement has traditionally kept its networked communications in a closed environment because of the sensitive information that police and investigators handle. Sensitive shared or networked communications are obviously not unique to law enforcement. 9/11 brought the critical interdependencies of industry and law enforcement to the forefront, especially what we now call “critical infrastructures,” such as the power grid, telecommunications, transportation, water, and so on.

**Jack:** How did this series of events lead to secure collaboration over the Internet?

**Kevin:** Presidential Decision Directive 63 had a large impact on my world view and I was determined to help build a secure online community where law enforcement, industry, the DoD community and academia could collaborate in a secure fashion. It was a great stroke of luck that I ran into a DARPA security professional, Bob Dowling, who introduced me to a DARPA manager, Matt Donlon, and a technocode writing wizard, George Johnson (with a background at the Software Engineering Institute at Carnegie-Mellon). These folks had built a secure online community prototype for industry security professionals called the Extranet for Security Professionals.

At that time, I was also serving as a moderator for the National Cybercrime Training Partnership on the FBI secure online system called LEO (Law Enforcement Online), created by a friend, Gary Gardner. LEO was successfully serving law enforcement, and the XSP was likewise serving industry security professionals. Recognizing the tremendous benefits that each of these systems brought to their users, I approached Matt Donlon and asked if he would be willing to help build a synergistic collaborative system for both law enforcement AND industry. Over a handshake, the Cybercop Secure Portal was built. Eight years and 11,000 users later, Cybercop is now fulfilling the dream of securely linking law enforcement and industry in pursuit of homeland security.

**www.cybercopportal.com**

Shortly following 9/11, I was approached by a friend and colleague who asked if the Cybercop Portal could help disseminate information to the WatchList community of more than 150 industry groups and businesses. Within 48 hours, all of those communities were enabled with their own secure compartment in the larger Cybercop Portal community.

**Jack:** How does a secure online system like the Cybercop Portal serve to enhance our nation’s security?
**Kevin:** As former National Security Advisor Richard Clarke has observed, “Security is community.” Retired FBI Profiler, Bill Tafoya, and I filled in at the last minute for Richard Clarke for the keynote address at the Blackhat conference two months before the 9/11 tragedy. During that keynote, we invited the industry-heavy audience to join with law enforcement in protecting our nation’s infrastructure. We emphasized that the “elite” are not those who attack and wreak havoc on the Internet, rather it is those who protect and defend the Net.

Conferences like TechnoSecurity (www.TechnoSecurity.com) bring a strong security-oriented community together for a week or so each year. The Cybercop Portal extends the collaboration reach of security professionals far beyond the fixed and rigid bounds of time and location. It’s effectively a 24/7 security community with a memory, and the ability to create secure compartments within the larger community within a matter of minutes.
This page intentionally left blank