

## 6

*Spy vs. Spy***Prologue**

It was a dark, drizzly, Halloween night. I drove along a typical suburban six-lane road, divided and lined with strip malls. All I was doing was looking for a place to buy some bottled water. The road was deserted and I drove slowly, looking side to side for a supermarket or convenience store that might sell water.

I passed a Wal-Mart but didn't feel like having to find a parking space and stand in a long checkout line. I was just tired and wanted to get my water and get in and out quickly. After another mile of closed strip malls and not knowing when I might see something that met my criteria, I decided that I might as well go to Wal-Mart.

I was driving well below the 45-miles-per-hour speed limit in the far-left lane of my three lanes and thought it would be easy to make a U-turn back to the store. I then glanced into the rearview mirror and saw a pair of headlights about three car lengths behind me. The car was just keeping its distance behind me, not trying to pass me, despite the fact I was driving slowly.

Unlike in the movies, the way to tell whether you are being followed is to drive slowly, not to weave in and out of traffic seeing who weaves with you. You want to see who doesn't want to pass you. In this case, instead of looking for the U-turn, I continued to drive 10 or so

miles below the speed limit and moved over to the middle lane to see whether the car would continue following me or this was just a coincidence. The car stayed behind me. It was time to assume that I was being followed. It had been more than a few years since I was last followed and I had to go through my mental checklist of what to do next.

Also unlike in the movies, you do not start speeding off when you know you are being followed. You continue to drive at a safe speed and distance until you can find a safe place to pull into. A “safe place” is one that is well lit, with many people, ideally with a way inside a building and a back door out. As luck would have it, a quarter mile up the road I saw a gas station with a minimart. I waited until the last moment to cut across the right lane and into the gas station. I then pulled my car up to the door of the convenience store with the driver-side door immediately facing the store’s door. My newfound friend followed me in.

I was slightly relieved when I saw a flashing red light go off on the dashboard of the car. I still waited to see whether my friend wore a real uniform. Not knowing what to expect, but with four or five other people now around, I got out of the car to confront the supposed officer.

“Can you tell me why you were following me?” I yelled.

He replied that I was driving below the speed limit.

“Since when is obeying the law now a cause for suspicion?”

I replied.

He commented that I crossed two lanes of traffic to get into the gas station. I told him that it looked as though he was following me, which he was, and that I wanted to get someplace where there were other people.

Being that it was Halloween night, and that it would not be uncommon for there to be a lot of drunk drivers, I couldn’t blame him for following the only car on the road. I showed him my hotel key and rental car agreement, and he felt comfortable knowing that I just arrived in town about an hour before and hadn’t had time to be on a drinking binge.

Little did I know that this would be typical of the week as a whole.

## **The Mission**

We were in a midsized town on the East Coast of the United States, performing an espionage simulation as part of a full-scope penetration test of a Fortune 500 manufacturing company. I led the team that also

included Stan and Tony. We were targeting one of the major facilities of the company. The primary target of the attack was the computer facility; however, the whole facility was fair game.

You probably wouldn't notice the people on my team on the street, which is what makes us perfect for the job. Stan is the Russian defector whom I mentioned earlier in the book. He was a full colonel in the GRU, the Russian military intelligence organization frequently described as the evil twin of the KGB, prior to his defection. He was one of the GRU's most effective spymasters in its history. Tony, who looked like an innocent country boy, was previously a military counterintelligence officer. Ironically, he was responsible for following Russian spies at one point in his career. I was to perform the black bag operations. Between the three of us, we had dozens of years of intelligence and security experience.

Stan, Tony, and I met for breakfast and I briefed them on our potential targets. I told them that we were supposed to meet with the security manager in his office in about an hour. The first task was to get to his office without his assistance. This was not supposed to be easy.

I was at the facility about a month before, when I was given a mini-tour. I knew that there was a gate around the perimeter of the facility, with guards stationed at the gate entrances. There were also guards at the entrance of the building we were focusing on. Getting into facilities guarded in this manner was my area of responsibility.

The plan was to try the direct route. I decided that on the first day we should take only one car. I timed it so that we would drive through the perimeter gate during the morning rush hour. As luck would have it, there were two lanes going into the facility. The guards stood next to the right lane, so we took the left lane. We went by the first checkpoint easily.

I parked near the primary target and we walked over to the building. The guard desk was to the left and in front of it was a table with temporary badges—the typical name tags that you write your name on, peel off the back, and stick on your shirt. There was an inner set of doors that required an access card to unlock. Of course during the morning rush, there were a lot of people going through, many holding the door open for the person behind them.

Not knowing what the process was, I walked over to the guard desk and said I was there to meet with someone. He told me to write my name on a temporary badge and he would buzz me in. He noticed

that I had a computer bag with me and told me I should fill out a form that logged in my computer. The idea was that someone would inspect my computer bag on the way out to see whether I was trying to steal a computer, but that inspection never happened.

I filled in the form with some fake information. I wrote my name on a badge and grabbed a couple of extra badges for Stan and Tony. I whispered to them to just tailgate behind someone else walking through the inner door. The guard told me that he would “buzz me in” when I walked over to the door, but that turned out to be unnecessary; I just walked in behind someone else.

I met Stan and Tony inside the door in a wide, long hallway. The Computer Operations Center, as well as the support staff and security manager, were in the basement of the building. I walked my partners over to a staircase that led downstairs. We arrived at the security manager’s office before he did.

We met to determine the specific tasks we would perform and also to set up a containment strategy if anyone “caught” us. Our primary target was access to critical computer servers, whose names we were given, as well as any information about future manufacturing plans. We were to also find out what other information was readily available to people who use hostile intelligence tactics.

Further breaking down the test, I was responsible for physical access to critical facilities. Tony would perform the traditional social-engineering activities, such as pretext telephone calls and open-source information gathering. Stan was to do what he did best: figure out how a traditional intelligence operative might find people to steal information for him.

We suspected that the company had experienced many espionage incidents in the past, and were formally told just that. There was indication that foreign governments sponsored some of the espionage, but much of it was sponsored by well-financed competitors. Stan’s experience was uniquely suited for the task.

## **The Black Bag Operation**

We decided to explore the facilities to get a feel for the environment. The basement was your typical Dilbert-style cubicle setting. Several large rooms opened into each other, with the exception of the Computer Operations Center, which was a large complex walled off from

the rest of the basement. There were a few strategically located doors with cipher locks that provided access to the computer rooms. Cipher locks are keypads that require the user to enter a code to unlock a door. The main computer room was about 75 feet by 200 feet, with long rows of computer racks loaded with equipment. Outside the main computer room were several telecommunications rooms where all the communications lines came in. There was also a control room at the far side of the computer room. That room had a large window looking into the computer room, as well as a door.

As we walked around the cubicle area, Stan commented on the fact that many desks had Chinese-American dictionaries on them.

“Have you seen the computer departments of U.S. colleges lately?” was my sarcastic reply.

“I’ll look into that,” was Stan’s matter-of-fact reply.

As we walked around, we found many unattended desks with the computers logged in, a great deal of valuable information lying around, and the typical messy desks that you would expect to see in computer environments. There were several people scattered around, so we really couldn’t look too carefully at any one desk.

When we got to a door to a computer room, we found it propped open, with cables coming out of the door. It turned out that major construction was going on, and the construction workers were using power from the computer rooms for their tools. We walked in the door and started wandering around. Nobody was working in the computer room. All the network administrators were in the control room. We had unchallenged access to everything.

To make the situation even better—for us, at least—the critical computers had their names taped to the monitors, and they were all logged in as the administrator. We had complete access to the systems we were told were our top priorities. If we had criminal intent, we would have added accounts to the systems and put in backdoors to allow us to gain remote access later.

I typed in some basic commands and quickly created a file in the administrator directory to prove we were there. We then quickly left and went back to the security manager’s office to regroup. The systems compromised held all the critical manufacturing plans and new designs for the company’s major product lines. Not only did we theoretically compromise all the current information, we would have been able to access these systems indefinitely to get any updates. This was about two hours into the test.

Everyone concluded that my black bag portion of the assignment was successful enough at this point. We had a feel for the environment and decided to move onto the other tasks. It was time to survey the outside environment, so we decided to leave for an early lunch.

We drove around to get a feel for the bars and restaurants in the area. Stan made comments about the Chinese restaurants that we passed. We finally chose a common chain restaurant. While eating, we took note of the types of people walking in and out and tried to determine whether they worked at the targeted company.

Returning to the facilities, we again had no problem driving in through the main gate and then following someone into the building.

## **Social Engineering**

Tony told us that he wanted to start making some phone calls to see if he could get user IDs and passwords from people. The week before, he started examining the company web sites and other publicly available information. He had collected dozens of names of employees, along with information about their locations and job functions. As do all Fortune 500 companies, our client had many locations around the world.

Tony started his calls by phoning the Help Desk and pretending to be an employee who forgot his password. The support person told him that she wanted his social security number to verify his identity. Tony told her his boss was coming and he would call back. He had all the information he needed at this time.

At that point, Tony knew he could call employees and either get their passwords or their social security numbers. He decided to try for social security numbers first, because it can be assumed that if people would give up their social security number, they would more than likely give up something less personally sensitive such as a password. Tony decided to say he was with the Help Desk and was investigating a security incident.

He began the call by asking users whether they had recently changed their password. Of course, nobody ever said they did. Tony then told the person that there was a security incident where someone pretended to be a user and changed that user's password. He said he would set it back to what it was, but he needed to verify the user's identity due to the nature of this problem. He then asked for the social

security number, and received it on all but one occasion. Having the social security number meant he could call the Help Desk at any time and have the password changed for his use. This meant that he would have unlimited access to just about any account he wanted. He compromised dozens of accounts over several hours.

Just to prove that it could be done, after going through his same spiel, he told some people that he could set the password back to what it was originally, “if you tell me what it was.” This way, he wouldn’t need to go through the Help Desk to access the accounts. He was always successful.

There was one woman who would not give Tony any information. She was the only person, out of almost 100, who did the right thing. Fortunately, or unfortunately depending on your perspective, it appeared that she didn’t know to whom she should report the incident.

## **Black Bag Operations, Continued**

I thought it would be a good idea to get shirts with company logos on them. Stan and I decided to try to find the Company Store, as it was called. It also provided us the opportunity to see whether the rest of the facility was as easy to get into as the areas we had already visited. Stan and I were told to find another building and given directions from the door to the store.

We arrived at the building and walked in the entrance, which was supposed to be an employees-only entrance. A guard was sitting at a generic desk to the side of the door. We just said, “Hi” and walked by him the way everyone else did. We found the Company Store, which turned out to be closed. In the process of walking over to the store, we found other things of interest to our mission.

We discovered that most of the buildings were connected to each other. We didn’t need to drive to another entrance, which was fairly far away. It also meant that the lethargic guard we passed allowed access to the Computer Operations Center, as well as to many other critical areas throughout the company’s research and development facilities.

After we confirmed we could make it all the way through to the Computer Operations Center, we had to go back and get the car. Along the way, we stopped at the bulletin boards where people could post advertisements. Mostly we found the names of people with their work telephone numbers. There were also several retirement

announcements, which contained the names of people retiring, as well as the secretaries to call to confirm attendance at the retirement parties. We passed this information back to Tony for use in getting more passwords.

At this point, we decided that Stan should go off to focus on finding places to recruit spies. Tony needed a break, so I took him with me to get back into the Computer Operations Center. This time, we wanted to get into the side rooms where the networking closets are. The side door we went in through previously was now closed. It was time to prove that it wasn't a fluke that we got in the first time.

Tony and I stood at main entrance to the Computer Operations Center, next to the cipher lock. I had a pad of paper and drew something that looked like wiring plans. We heard someone coming from inside, so I pretended to start entering a code into the lock. As the person came through the door, I acted as if I had just finished entering the code, and Tony and I thanked the person for holding the door open.

Once inside, we saw a hallway. The door to the Computer Operations Center was on the right, and we just walked straight down the hallway. To the left and at the end of the hallway were the network and telecommunications rooms, whose doors were wide open. We didn't notice anything too unusual. We did, however, confirm that we could have tapped the telephones and networks.

Later, we did a late-night walk through the support areas outside the Computer Operations Center. There were passwords lying around, sensitive information sitting on desks, and terminals left logged on, some of them with administrator privileges. However, the most notable thing we found was a very large computer printout. This printout contained a list of all employees with a variety of their personal data, including their social security numbers.

As far as black bag operations, I was pretty much finished. There was little more of value I could prove. Tony continued to make his telephone calls, getting password after password. He ended up leaving early. Stan, on the other hand, found other things of interest, to put it mildly.

## **Spymaster at Work**

Stan went to several bars located around the facility. He found out that there was a major competitor in the same city, which wasn't any secret.

Talks with bartenders uncovered that certain executives of our client frequently met with executives of the competitor. The bartenders said that they spoke very secretively.

At some of the seedier bars, Stan found many people who were drinking excessively at lunch. It wasn't hard to figure out that people drinking heavily during lunch were not very enthusiastic about the company. This was a spymaster's ideal hunting ground.

Stan also went to different restaurants to see the clientele that they attracted. Stan determined where the younger people who might want some excitement would go, where the older disgruntled people would go, and where spies would avoid.

Because this was in a post-September 11 world, Stan also decided to see how alert the company was to potential terrorist threats. He drove his car up to the primary building we were targeting, and then got out and left the car. It was even in a fire lane. He watched from a distance for 15 minutes and saw that no one even came out to check the car. That was more than enough time for a terrorist to get far away and have the car explode. He got back in his car and drove off.

Stan wanted to check whether the apathy with his car was due to the trusting Southern hospitality or unique to the guards at the company. He drove over to the competitor's facility to see whether he could leave the car in front of one of that company's buildings. He found that it was actually physically impossible to drive right up to a building. There were at least 50 feet from any road or parking lot to any building.

Sometime during Stan's travels, someone apparently noticed him. Much as I experienced two nights earlier, Stan detected someone following him. To confirm this, he turned on to one deserted road, then to another and another. Stan is a true master at this, because there have been many times that his life depended on surveillance detection and avoidance. When Stan reported this event to me, he made it a point to say that the people following him weren't very experienced. When I asked how he knew this, he said that there was only one car. A professional operation uses at least two cars, and even one car would have been less obvious. More important: "I made a U-turn on one of the deserted streets, and the car hit a signpost as he tried to follow me," he said with a smile.

Stan and I hypothesized about who it could have been. The options were a Russian spy who recognized Stan and wanted to see what he was up to, an FBI trainee doing counterterrorism work who

thought Stan might have been a terrorist scoping out the companies, or possibly security from either our client or the competitor. Given all the valuable information that the company has, and the previous cases of espionage, we were certain that a variety of foreign intelligence services target it on a regular basis. There were definitely spies among us on this assignment.

Stan's experience as a GRU spymaster became a major factor. With the exception of his final stationing in the United States, the rest of his GRU career was focused on China. He was even stationed in Beijing for four years.

Even knowing this, I was still confused by a call I got from Stan a day later. "Ira, there are black duck eggs on the menu," was his cryptic comment.

"Stan, what the hell are we paying you for?" was my reply.

"Oh, my naive American friend," he said with a smile I could feel over the telephone, "black duck eggs are a Chinese delicacy. I can hardly find black duck eggs in San Francisco, let alone this little piece of s--- town in the middle of nowhere. And they're cheaper than they are on the streets of Beijing."

He went on to describe that because he saw all those Chinese-American dictionaries on the desks of the employees, he spent some time trying to find Chinese social clubs and other places where Chinese people may congregate. Stan knows the modus operandi of Chinese intelligence agents, which is to find people of Chinese descent and sift through them to see who would likely be susceptible to recruitment. Generally, these are people who have more allegiance to China than their employer or who can be coerced because of family in China. Setting up a gathering place, such as a Chinese restaurant that has hard-to-find Chinese delicacies, is a way to attract as many potential agents as possible. It is also a great place to exchange information and money.

Stan told me that he found several Chinese restaurants reasonably close to the company facilities. All but one had friendly staffs that welcomed him. At the other, he walked in and saw a menu on the reception table that had only Chinese writing. He picked it up and saw that there were Chinese delicacies not normally found in other Chinese restaurants in this country. When one of the workers realized that Stan could read Mandarin, he became distressed rather than gladly welcoming toward the potential new customer who could appreciate the rare menu items.

Stan's being followed was a fact. Whether or not this Chinese restaurant was actually one of the more than 3,000 Chinese front companies was a matter for the FBI. Stan was told that the FBI was busy doing counterterrorism work; the investigation of the restaurant was a low priority.

## **Case Summary**

All the penetrations were finished within four days. However, my black bag operation could in fact have been declared successful and complete within four hours. Tony's work gathering user account access from all over the company was successful within two days. Stan's work took approximately four days and could have lasted longer.

Tony and I proved that if someone wanted to compromise the company, he or she could do so very quickly. Many people want to believe that although the vulnerabilities exist, nobody would really exploit them. Stan's work proved that it was extremely likely that there was at least one well-funded espionage operation targeting the company, and likely many more.

Even worse, Stan confirmed his own concerns that dozens of people in the computer support group were targeted. Not only that, this prime *and actively targeted* population had access to the most valuable information in the company.

Although most people appreciate that these types of results can happen at most companies, some people say it was just luck. My team has this type of luck on all our penetration tests. Espionage is about taking advantage of the opportunities that present themselves. If it hadn't been construction work that enabled us to get into the Computer Operations Center within two hours, there would have been another opportunity. Trained spies know how to be where opportunities present themselves, as well as how to recognize those opportunities. It is like the old saying, "Of course I believe in luck. It seems like the harder I work, the more luck I have." In this case, the work is training to quickly and effectively recognize and exploit vulnerabilities.

A few people question whether there would even be a Chinese intelligence operation to be found. They don't believe that these things happen in real life. Maybe a Chinese restaurant would ship in expensive items to sell at a large loss so that it can sell more of these items for more of a loss. People believe that these are things only for spy novels,

not real life. The real spies love and rely on this ignorance and cynicism because it means that people will continue to ignore the vulnerabilities and the spies can continue to exploit them.

## **Vulnerabilities Exploited**

When I tell people about this case, many swear that it is their company my team attacked. If not, they say that the same thing could have happened at their company because they have the same vulnerabilities.

The vulnerabilities exploited in this case were primarily operational ones, which makes sense because this was primarily an operational attack. There were also technical vulnerabilities discovered in the process.

At this point, I do not mention countermeasures in detail. Clearly, you should be able to infer security procedures that could have stopped the attack. As I said in the beginning of this section, the vulnerabilities exploited were small and usually obvious ones that should have been stopped by countermeasures in place. However, this case demonstrates that people take the obvious for granted.

### **Ineffective Perimeter Security**

The fact that we were able to drive right past the guards at the perimeter gates, just by acting as though we knew where we were going, made the gates useless. Maybe they would have tried to stop a large truck, but consider that multiple cars could accomplish the same amount of damage that a truck could. At the very least, the guards could question visitors and announce their presence to the people being visited. As it was, the guard booths were just information booths.

### **Poorly Trained and Monitored Guards**

There were clearly security procedures to be enforced. Guards should have been watching for people tailgating others into the facilities. The visitor badges shouldn't have just been sitting there for people to grab by the handful. I did fill out a form to register my PC, but no one checked my computer bag on the way out. The guards were too far away to stop me if they wanted to. The one guard we just walked by was useless except to people who needed directions. Stan's leaving his

car right next to the building's entrance should have warranted a very quick reaction. The fact the guards didn't even care about a fire lane's being blocked, let alone the potential terrorist action, is the most telling sign of learned apathy.

It is easy to blame the individual guards for the lapses. However, in reality it is a management problem. The company acted as though just having a uniformed body were enough. They clearly did not go through enough effort of training the guards, or at the very least, spot-checking them to see how well they performed their job. Thousands of people go by the guards and their posts on a daily basis, and they should notice the same issues that I did. However, no one took any actions. It is not the fault of the individual guards if this seemingly apathetic behavior is accepted.

### **Poor Construction Procedures**

Strong security countermeasures were in place at the company, such as cipher locks on doors to the Computer Operations Center. However, the construction situation allowed someone to prop a door open. I mentioned only one instance of this here, but there were many others. Any spy would jump on these types of opportunities.

Also, spies could easily get jobs on the construction teams. There were no background checks on the construction and support workers, and they pretty much had unimpeded access to the entire Computer Operations Center and surrounding support areas. They had more access than the regular employees of the company. As a result of our test, the company spent several hundred thousand dollars doing a bug sweep and searching for other network and voice eavesdropping devices. Although this would be a good idea anyway, it would not have been as necessary if they had controlled the construction team.

### **Lack of Escorts**

One control that should have been in place is escorts for any visitors to the basement. Not only could this prevent abuse or criminal activity by the construction team, it would have cut down on other outsiders' ability to gain access to the Computer Operations Center and similar areas. For example, the escorts likely would have prevented doors from being propped open.

The construction workers would not question other people following them into controlled areas. That is not their job and they wouldn't know who belonged and who didn't belong, anyway. Escorts could have been told to question any unescorted person who was not authorized in controlled areas. This would likely have prevented our unfettered access to the Computer Operations Center. Although a trained spy or other criminal is not likely to be put out of business by the mere presence of an escort, it would discourage professionals from planting bugs or stopping at an unattended computer terminal. It might even catch the amateurs, of which there are many. The escorts should also have prevented doors from being propped open.

### **Easy Entrance to the Computer Support Floor**

Even though the Computer Operations Center itself had cipher-locked doors, the support areas surrounding it had no protection. During our walk-throughs of these areas, we found more than enough information to be successful without getting into the Computer Operations Center. Many critical computers were left unattended and logged on to administrator accounts. Although those issues need to be addressed individually, the fact is that anyone with access to the building as a whole had complete access to the support area. Remember also that we found that several buildings were interconnected, which compounded this problem. As a result of the test, cipher locks were installed on all staircases that led to the basement.

### **Computer Terminals Not Locked**

Computers in the Computer Operations Center and support areas were left unattended and logged on to administrator accounts. This meant that anyone with physical access to the facility had the ability to take complete technical control of all critical computers—a one-time compromise becomes an indefinite compromise. If screen-locking mechanisms were enabled, these compromises would not have occurred.

### **Telecommunications Closets Not Locked**

Telecom closets are basically the spinal cord of a company. If you have access and the technical knowledge, only encrypted communications (which are rarely used, especially for voice communications) could stop

you from accessing information through the communications lines. Anyone could have easily tapped into the communications lines for the Computer Operations Center. A password sniffer placed here gives an attacker all the account passwords for everyone involved in research and development, along with their data. These closets should be tightly controlled and always locked, unless they are attentively attended.

### **Use of Social Security Numbers as Employee Identifiers**

Although you need unique identifiers for employees to prove their identities, social security numbers are clearly not a good choice. In the first place, it might be a violation of local privacy laws. Also, social security numbers are easy to get. If you find out that someone works at the targeted company, you can get that person's social security number off the Internet. You can then call the Help Desk and claim to be that person, without ever needing to contact the person directly.

### **No Knowledge of to Whom to Report Incidents**

During Tony's social-engineering attacks, only one person out of almost a hundred refused to give him her password. This person knew that the request as a whole was a violation. Immediately after this incident, we alerted the security staff that the person should contact them about the incident. The call never came, and when we looked into it, we learned that the employee had no idea whom to tell about the strange call. So even when people did detect something unusual, they didn't know the appropriate steps to take about it.

### **Poor Security Awareness**

The fact that Tony was able to get so many passwords indicates that the company as a whole had poor security awareness. When only one person out of a hundred does the right thing, poor security awareness is a management problem. The success of the black bag operations also proved the poor security awareness endemic throughout the company.

### **No Challenge of Strangers**

Despite the fact that Stan, Tony, and I walked all over the company, past guards and hundreds of employees and into sensitive areas, nobody

challenged us. We were clearly not personally known to anyone in the company except a small project team. We never put on those stick-on name tags because that would have aroused more suspicion than not wearing badges. At a minimum, we would expect to be challenged three or four times, at least by the guards that we passed. Although this is a symptom of poor security awareness, it is important to highlight because it is common in many companies.

### **Tailgating**

As noted, tailgating is something the guards should have noticed. But the people who allowed us to tailgate them are also at fault. It's another sign of poor security awareness that we were able to follow people into a controlled facility, such as the building, without their looking to see whether we had a badge or an escort. This means that despite millions of dollars of strong physical locks, anyone can get into the facility. Office pirates use this technique to enter offices and walk out with computers.

This is important not only for information security but also personal safety. Outsiders can walk in and physically assault people. In one case, I was called in to perform a security assessment after an estranged husband walked into a facility, following behind others who held the door open for him, and shot his wife.