CSI: Humanity
(Computer Security Investigation)

Rebecca Herold, CIPP, CISSP, CISA, CISM, FLMI

Final Draft for September 2007 CSI Alert

At night things seem very different. I enjoy going outside after the sun has completely set dark. You hear sounds you never hear in the daytime. You see things you never see or notice during daylight. It's not much different within the workplace.

In 1990 when I was an internal auditor I was tasked with determining the overall information security posture of the company. One of the things that I decided would be a good thing to do was to go to the offices Saturday and Sunday evening when there would be the fewest personnel around. I wanted to look at their work areas to see what type of information security risks I could find that were a result of the work habits of the personnel. A computer security investigation for the human realm. Oh, boy; it was an eye opening experience! I found so many vulnerabilities it filled pages. It became a significant basis for what would become the organization's first set of information security policies. Over the years I have refined the process quite a bit.

Doing after-hours walkthroughs are a great way for all organizations to get out where their personnel work and see what kinds of risks exist to information when no one is around. They can usually be done during the work-week within specific business areas in around two to four hours. Partnering with the physical security department and having them come along increases the time investment value and security value greatly by not only having physical security risks identified at the same time, but also giving the information security folks a chance to raise information security awareness for the physical security folks and vice versa.

Some people have said to me over the years, "But the risks are so little at night! No one is around, with the exception of the security guards, cleaning staff, maintenance workers and employees who may be working late." Yes, these folks very well COULD be in the area. I have seen many instances of security guards doing bad things with the information they have found, along with the cleaning staff, maintenance workers and employees. When you think about it this is a very large number of people, isn't it?

What are the information security and privacy vulnerabilities you are likely to see? The possibilities are endless! Here are eighteen common vulnerabilities, in no particular order, to get you started in thinking about the possibilities. Add to this list and create a walkthrough checklist based upon it to log what you find.

1. Computers logged into the network and unlocked

There inevitably are computers found that are still logged into the network and that have not been secured. Don't let the presence of a screensaver fool you. Move the mouse or touch the mousepad and see if the computer is still logged into the network. Just think about all the things a malicious person could do through the authorized access of your IT administrators, your HR workers, your accounting department personnel, your information security staff (yes, numerous times information security personnel

themselves leave huge vulnerabilities in their work areas), and other folks with access to sensitive information.

2. Passwords written and easily discovered
It seems passwords have been written on sticky notes since the introduction of Post-its in 1968. You will often find computer passwords on notes stuck to the computer monitor, under the keyboard, on the desk calendar, on the overhead bin, and under tissue boxes. You will find voice mail passwords on notes stuck under the phone, etched into the phone handset, and also nicely labeled under the keyboard. I've found many password tokens with the PIN number written on, and even scratched into, the token itself.

3. Negotiable checks out in open
If you work in an organization that receives payments from your customers, look in the accounts receivable and accounting areas for checks lying out in the open for anyone to pick up and walk away with. There is an amazingly large amount of information on checks that can be used to commit identity theft and other types of fraud. Probably one of the most egregious cases I found was when in an otherwise amazingly clean and tidy desk area that processed real estate payments. There was a very tidy stack of negotiable checks stacked neatly on the keyboard propped against the monitor. The checks, around 30 of them, were all for tens of thousands, and a few for hundreds of thousands, of dollars each. The employee explained she did this every night before she left so that she could get a "quick start" on processing the checks first thing in the morning.

4. Papers with sensitive information on desktops
It is amazing the amount of sensitive printed information that is left out in the open on top of desks. Much contains customer personally identifiable information (PII) as well as employee PII. One of the worst cases I found was within a director's office. He had, in very neat stacks on his long desktop, all his direct reports' personnel files laying in front of their corresponding "Confidential" envelopes. The employees' entire payment history, managers' notes, beneficiary information, social security numbers, and all other information, available for anyone to see who would walk into the office, which had the door wide open.

5. Unapproved network connections
At one of my clients, one of the server administrators in a business unit with many different business partners did not like to be slowed down by rules and was always agitated when told to follow the procedures. He always wanted to set up connections to his networked server from the other companies himself. "I could easily set the connections up myself," he would say. Turns out, this admin knew that network cables ran in the ceilings above the dropped ceiling panels. Apparently, sometime when no one was around, he had removed the panels above his cubicle and examined the wiring long enough to identify where to patch in a cable, from a modem that was on his desk, to his server. The cable ran up the wall, and was hidden by a tall voluminous fern, which we discovered during one of our after hours reviews. Look for suspicious connections to computer equipment and wiring.

6. Unapproved software

There have been numerous times when I have found software boxes, CDs and diskettes in personnel work areas that have brought in and installed on employee computers, and even on the network, without approval. Some of the more clever folks install the software for the time period they want to use the application, and then uninstall the software in an attempt to thwart the corporate software inventory tool. If they are using the software to create business materials or products this could put your organization into jeopardy of licensing noncompliance. And then there are the malicious code risks. Look for boxed software packages in addition to CDs and diskettes out in the area. Oftentimes you will find the CDs and diskettes clearly labeled with the application name.

7. Unapproved access points
Believe it or not, modems are still being used to circumvent access into and out of the network. I've found several instances of employees who used splitters, widely available in electronics stores, to allow their phone lines to also be used on their computers. Note any external modems in the areas, or if you see phone cables hooked into the computers. Look for signs of wireless installations as well.

8. Sensitive information in trashcans
Look in your personnel's trashcans and in the big trashcans for the department. What type of papers and other items are there? Just as throwing food into trashcans attracts roaches and rats, throwing away sensitive information attracts dumpster divers and criminals. It also attracts people who want to retrieve the papers to use for scratch paper within their schools, churches and clubs, which has resulted in privacy breaches many times.

9. Sensitive information in mail slots
Don't forget to look in the mail slots for each area to see if there are blatantly sensitive information available for the taking. It is very easy for someone to take information from the mail slots and make a copy of it at the usually near by copy machine, and then put the information back into the mail slots. The intended recipient will never know that copies were made and could now be in the wrong hands.

10. Sensitive information in printers, copiers and fax machines
People often forget to take their originals from the copy machines, or leave some copies in the tray. Even more often, people print email messages or reports with sensitive information, get sidetracked, and then forget to go get the printouts. People often send sensitive information within faxes to others without notifying them, leaving the physical fax machines holding confidential information for anyone passing by to pick up.

11. Keys in desks and filing cabinets
It is very common to find keys sticking out of the key locks in desk drawers and filing cabinets. When they turn up missing people usually don't give it a second thought, thinking they have misplaced the keys, and end up getting copies made. Meanwhile others may have those keys to use when others are not around.

12. Open doors
I have found many doors to stairwells propped open with trashcans and boxes. While I was in a location in the information security area on the 16th floor of the downtown

building there came a woman through the stairway door with her three small children in tow. She saw me and the others in the nearby office talking, came over and asked us how to get to the downtown Walgreens. Unauthorized people who easily got into a restricted area. I have found doors to computer operations rooms held open with broomsticks and umbrellas. Usually people have propped them open with every intent of closing the door after they have carried something through, but it is very easy to get sidetracked once crossing through the doorway, leaving the door open for anyone in the area to walk through.

13. Mobile computers unsecured
It's funny how mobile computers have a tendency to walk away "on their own" if they are left unattended and unsecured. Mobile computers of all types are attractive targets for thieves who want the data on them or the hardware itself. Mobile computers are reported stolen or lost every day, and those reports represent just a small fraction of the actual losses.

14. Mobile storage unsecured
There are so many types of data storage devices out there. It is easy to copy many megabytes of sensitive data onto any number of them and then carelessly leave them out in the open. Most of the data on these devices is not encrypted. Look for USB storage devices, in all shapes and sizes, along with DVDs, CDs, diskettes and even MP3 players and smartcards.

15. Confidential information in meeting rooms
White boards and flip charts are commonly used within meeting rooms to discuss plans and make decisions. When the meeting is over and another group is waiting to get into the room for the next meeting, everyone often jumps up and leaves without erasing the white boards or tearing off the flip chart pages. I have found information such as disaster recovery team member contact information, data flows and corporate plans that would be very valuable to competitors.

16. Outdoor trash bins with confidential information
You would think after years of talking about the prevalence of dumpster diving that people would not be throwing sensitive information into outdoor trash bins anymore. However, it seems to happen daily. Just this afternoon (8/10/2007) it was reported that documents including 2006-2007 sophomore students' TAKS score sheets, a listing of the senior class rankings by grade point average and several folders with student PII were found in a dumpster behind the Waxahachie High School in Texas.

17. Unlocked storage rooms
Almost every time I do an after hours walkthrough I find unlocked storage rooms with printer-paper sized boxes, usually very clearly labeled with the type of information within them, on shelves. Often they are customer account information or employee information archived into the boxes and into the unsecured room. Tons of PII, all in one easy-to-carry box for someone who would like to use the information for criminal purposes, or sell it to lots of other criminals for a nice profit.

18. Unsecured mailrooms

Medium to large sized organizations often have their own mail areas with staff dedicated to processing the mail. Think about the huge amount of confidential information that is sent through postal letters, packages, UPS, FedEx, DHL and other delivery services. Unsecured mailrooms allow for confidential and sensitive information to be taken, often without the recipients even knowing they were sent. Unaccounted for stolen mail can easily end up being the root of untraceable and unsolvable crimes and frauds.

There are many more types of information security risks that personnel can create within their work areas, but this should give you a good idea of where to start with doing your own after hours security walkthroughs. Just go visit your HR, customer service, call center, IT, Marketing and executive offices. Stand and look around the work areas for a while. Pretend you are playing Where's Waldo, except you're searching for security and privacy vulnerabilities. I am confident you will be able to add to this list of eighteen.

Reasons to do walkthroughs

- **To discover vulnerabilities**. This is the most apparent reason. You need to know the vulnerabilities to fix them.
- **To raise awareness**. You need to know what people are doing to put information at risk so you can address it with appropriate awareness and training. The reports you create from doing the walkthroughs are great eye-openers and significantly raise awareness.
- **To establish and maintain ongoing metrics**. Keeping track of the vulnerabilities found on an ongoing basis is very valuable. You can use the numbers to show risk trends and validate security program efforts.
- **To demonstrate due diligence**. Documenting the vulnerabilities, along with your reports about the results of walkthroughs and documenting the actions the areas will take to reduce the risks, provides powerful evidence that you are following a standard of due care in your data protection efforts.
- **To improve your information security and privacy program**. Not only do walkthroughs allow you to identify topics that you need to provide more training and awareness about, and the impact of your training and awareness, they also show departments and areas that are creating the most risk to your business

Remember to…

It is important to have executive leadership support for these walkthroughs. Do not try to perform them without speaking to your CEO; you could end up with some very angry middle management complaining to the CEO that they were blindsided. It is best to ask your CEO to issue a memo to all managers talking about the walkthroughs at a high level, and how they are being done to help improve information security and privacy practices. The memo should state that the walkthroughs will be done periodically within the business units, but it is usually best to not specify the exact dates. This way you will be able to see how the areas really look on an ongoing basis.

Following each walkthrough write a report summarizing the results, along with what needs to be done to reduce the identified vulnerabilities. Include your metrics to show how each specific area has improved, or worsened, since the previous walkthroughs.

Include copies of all the detailed log charts your created during the walkthrough with the report for the area's manager so her or she can address specific vulnerabilities with specified individuals. These results can also be incorporated into the annual performance appraisal.

Also consider publishing a yearly summary of the results of the walkthroughs to your board of directors and all your staff. This will demonstrate just one of the proactive ways that you are trying to protect the organization's information assets.

Performing walkthroughs was a good thing to do in 1990, and it's still a very good thing to do!

Rebecca Herold, CIPP, CISSP, CISM, CISA, FLMI is an information security, privacy and compliance consultant, writer and Norwich University MSIA adjunct professor. She just released the quarterly employee awareness tool, "Protecting Information" (Information Shield) and blogs daily at http://www.realtime-itompliance.com. She can be reached at rebeccaherold@rebeccaherold.com or http://www.privacyguidance.com.