Global Information Assurance Certification Paper

Information Security for The Mobile Legal Professional

Samuel Kaplin

GSEC Practical 1.4c Option 1
January 25, 2005

Abstract:

This paper was written as a nontechnical discussion piece for the legal professional who is working outside of the office. This may be at home, in a courthouse or anywhere the IT staff is not present. It's written from the perspective of an IT Professional who wants to keep his mobile users happy, productive and functional in a secure manner. This document isn't a definitive piece of research, it was written to foster the discussion of information security topics and processes in areas where the user is most vulnerable, when they are away from the policies and procedures of the physical office. If I can get two attorneys to talk about this paper, I'll deem it a success.

I've titled this paper "Information Security for The Mobile Legal Professional." It is an information security paper, not a computer security paper. In the legal community, much of the information resides in paper documents and files. In the Physical Security section we'll examine ways to keep your paper documents and your computers physically safe. In the Computer Security section we'll examine ways to keep the data on your computer safe.

Author's Background:

Now we get to the fun part, let's talk about me. In a previous life, I specialized in "Electronic Security." This means that I installed, fixed and maintained excess control systems, intrusion detection systems and video surveillance systems. Amazingly this has provided a very well rounded background for my current career.

I currently work for a U.S. governmental agency which exposes me to Attorneys, Judges and other legal professionals on a daily basis. I'm their "Tech Guy." I keep the workstations, servers, network, A/V equipment and anything else that uses electricity up and running. This allows me to watch lots of legal proceedings and see lots of information security lapses during those proceedings.

1 Physical Security:

1.1 The Shhhh Factor

As the old saying goes, “Loose lips sink ships.” This is more true today than it was in 1940. We have ears all around us. Some we can see, others we can’t. It’s up to us to keep confidential information confidential. Anytime you have an unknown person within an earshot there is the possibility of an unintended disclosure.

One day, my presence was needed in a courtroom. There were three other people waiting for the elevator with me. Two of them were obviously attorneys that were working on the same case. They were actively discussing their strategy. All four of us got in the elevator. Their discussion continued in the elevator during the ride up. The other quiet person in the elevator had a wry little smile on his face. We all got off on the same floor, and proceeded to the same courtroom. That’s when it hit the “gabby” attorneys. They had just outlined their complete strategy in front of opposing counsel. I’m not sure what impact this had on their case, but I can tell you it probably wasn’t good.

Sometimes you can’t even see the person listening. In a lot of courtrooms the audio is distributed to other areas of the building. If the audio system is on, it is entirely possible that someone in the Judge’s chambers may be listening to your conversation. Keep that in mind the next time you’re setting up for a trial and something goes wrong.

The moral of this story is to only discuss confidential information in secure areas. The hotel bar, restaurant or public elevator is not a secure area. Once the genie is out of the bottle, it usually can’t be put back in.

1.2 The War Room

It’s a very common practice for legal teams to set up a “War Room” for long trials in space close to the trial venue. Sometimes it’s a suite at the hotel. Other times it’s space in an office building near the courthouse. In this section we’ll look at the minimum physical security requirements for that space. The main goal is to keep your documents, personnel and computers safe and sound.

1.2.1 Locks

The first thing the space should have is a high quality lock on each door and opening window. The lockset should be from a major manufacturer. Upon moving in, your first action should be to have the locks rekeyed by a reputable locksmith. It is important to know who has keys to your space. It is entirely possible that a prior tenant may still have a key. The rekeying process mitigates this risk. It is also important that you use the locks on your doors and windows. The best lock only works if you use it.

1.2.2 Intrusion Detection

Hopefully your space already has an intrusion detection system installed in it. If it doesn't, you should seriously think about having one put in. Most manufacturers make reliable wireless systems now. The wireless technology should help reduce the cost of installation. If the space already has an alarm system, change all of the arming and disarming codes immediately. If the system uses keys, have them rekeyed as well. This is the only way to guarantee that only authorized users have the ability to arm or disarm the system.

There are two basic types of intrusion detection systems, "Local" and "Monitored." A local alarm system just signals at the premise. Its design intent is that the noise and lights scare away the intruder and call attention to the situation. It does not automatically signal a remote site for help.

A monitored alarm system has all of the bells and whistles of a local alarm system plus it calls to a remote site for help. Most monitored alarm systems use a phone line to call for help. Smart burglars will usually cut the phone lines to the building if they are accessible from the outside in hopes of disabling the alarm system's communication. Some higher security systems use a radio or cellular phone transmitter as a backup means of communication in case the phone line goes down.

A local security system may be adequate if the space has staff or a security guard present 24/7. If it doesn't, a monitored system is the way to go.

The false alarm has always been the bane of the alarm system. Sometimes things aren't as they seem. Criminals will sometimes intentionally trip intrusion detection systems to test their response. If the police show up a few minutes after they trip it, they know it's monitored. If they trip the alarm a few more times, perhaps the police or security will ignore it. Ideally the alarm should only be able to be triggered from outside with visible damage, for example a broken window or door.

False alarm attacks can be as simple as rattling a loose door or window. Or they can be as complex as using HAM radio equipment to generate radio frequency interference to make the alarm control panel misbehave. Some older Passive Infrared Motion Detectors are susceptible to having their infrared detector overloaded. The attack involves shining a 1,000,000 candle power spot light on the motion detector from the outside. Most modern motion detectors are now immune to this attack, but there is still a lot of old equipment out there. You should treat every alarm as if it were real.

1.2.3 Safes

If your "War Room" is in a hotel, I would be dubious of using the in room safe to store anything of value. Recently I had a chance to see first hand how insecure they really are. The battery on the safe in my room had gone dead. My laptop, MP3 Player and other vital

items were locked within. The front desk sent a maintenance person and two security people up to my room. The maintenance person arrived with two very common tools. Ten minutes later the safe was open and fixed. His procedure opened the safe and did not require an entry code reset on the safe. If I hadn't been in the room, I never would have known that the safe had been open. To add insult to injury, the security staff never asked me for an ID.

If your "War Room" is in an office space, consider purchasing or renting a safe. Typically the three major considerations when purchasing or renting a safe are size, fire resistance and burglary resistance. The safe should be sized to accommodate all of your records and items of value. In the fire resistance and burglary resistance category, you should buy or rent the best that you can afford. The safe is of little value if it can be easily removed from the premises. If the safe you purchase or rent is physically small, consider affixing it to the building's structure in some way. Most small safes have this capability designed into them.

1.2.4 Fire Suppression

Most hotels and offices have some form of fire suppression. Usually it takes the form of a sprinkler system. The way a sprinkler system works is very simple. A piece of metal melts or a vial of liquid shatters when the ambient temperature around the sprinkler head exceeds a certain value. This opens up an orifice in a pipe filled with pressurized water. The water then comes out of the orifice and hits a deflector which shapes the stream of water into the desired pattern. The water then hopefully extinguishes the fire. Papers, electronics and other items should be protected from water damage. Your safe or water tight plastic tubs should be adequate for this task. The tubs can be used instead of "Banker's Boxes."

Some sprinkler systems are configured to signal a remote location when the water begins to flow. For most systems this is critical because the water will continue to flow until a valve is manually turned off. This is very similar to the operation of a monitored intrusion system as discussed previously. If the two systems exist at the same facility, they may even share the same control panel and communication system.

1.2.5 Closed Circuit TV

Many office spaces have Closed Circuit TV (CCTV) cameras in common areas. The images from these cameras are usually sent to a location where staff may monitor them. This may be on the premises or off site. The system is only effective if someone is looking at the screens or the images are being saved to some sort of storage medium. This typically takes the form of a VHS tape, although digital storage is becoming more popular. One critical factor is the retention time of the media. Many places use the same tape day after day.

Recently, I had to pick a daycare center for my child. All of the centers I looked at had CCTV cameras installed in the rooms and the monitors were located in the Director's office. None of the facilities were saving the images to any sort of storage media. When I asked

why not, all of the facilities responded that they weren't doing it for "Liability Reasons." In other words, they wanted to be able to say they have cameras in all the rooms, but didn't want the liability if the cameras actually record something untoward. The moral of this story is that a CCTV system is only of value if someone is looking at the monitor or if the images are being recorded and retained.

1.2.6 The Impact of a Physical Loss

> *"James E. Blatt, appointed by the judge to oversee the police investigation of the burglary, said after the hearing, "Certain items were taken that could have a very negative effect if they get in the wrong people's hands."* [1]
>
> *"Schwartzbach declined to comment on whether he had copies of the material on the computer missing from his Sherman Oaks apartment, which was serving as his office."* [1]

These two quotes were from a CNN article regarding the theft of computer equipment from M. Gerald Schwartzbach's apartment. Mr. Schwartzbach is Robert Blake's attorney. For those not following the case, Robert Blake is accused of murdering his wife. It's a very high profile case due to Mr. Blake's celebrity status.

The quotes illustrate why it is critical to physically protect our information. Was the break in related to the case? At this point it's impossible to tell, but it could be. Did the loss of information affect Mr. Blake's case in an adverse way? It probably will. If Mr. Schwartzbach doesn't have current backups, the case documents on the computer will have to be recreated which will be a time-consuming process. Some evidence may not be able to be recreated.

Confidentiality is a cause for concern as well. Suppose the thief releases the case documents to the press. Will Mr. Blake get a fair trial then? Suppose the case documents were surreptitiously sent to the prosecution or police. How would that impact the trial?

This unfortunate event illustrates how important physical security is to information security. Once unauthorized parties have physical access to information, you can never be sure who has the information.

[1] http://www-cgi.cnn.com/2004/LAW/12/02/blake.wifeslay.ap

2 Computer Security

2.1 The Basics

In this section we'll outline some of the basic policies and procedures you should observe to keep your computer and information safe and sound when it's not under the watchful eye of your IT department.

2.1.1 BIOS Password

The computer should have a BIOS password installed on it. A BIOS password is a password which comes up before the computer boots or before any BIOS configuration changes can be made. If this is enabled, the computer will not start up without entering the password.

If you enable a BIOS password on your computer, and one day it is gone or the password no longer works this can be an indication that the computer may have been tampered with. Some computers have to be opened up and have a jumper shorted on the motherboard to reset their BIOS password. Some computers, especially laptops require a utility to be run on the computer to recover the password. Some manufacturers have a back door recovery password built into the computer.

The BIOS password, like any computer security item should not be viewed as secure unto itself. It is one hurdle of many that an attacker must overcome to get your information. To quote the folks at techfaq.com:

"The BIOS password can be reset on any system. Some systems are easy, others are more difficult. Any BIOS password can be reset with sufficient time, money and effort." [2]

2.1.2 Virus Prevention

Every computer should have anti-virus software from a reputable company installed on it. New threats come out almost daily. According to BBC news, at the end of 2004 there were more than 100,000 virus threats out in the wild. This is why the anti-virus software on your computer must be kept up to date. As new threats come out, the anti-virus software companies update their software to detect them. Most flavors of anti-virus software have an auto-update feature. When the software detects that you have internet connectivity, it will fetch and install the updates automatically for you. I would highly recommend turning this feature on.

---

[2] http://corky.net/2600/computers/reset-bios-password.shtml

A virus scan should be run on computers at least once a week. Sometimes a computer may become infected with a new virus before the anti-virus software company has updated their product. In this case the infection would go undetected by the real time virus protection. Before you run the scan, it is advisable to update your virus signatures to the most current ones offered by the anti-virus company.

If your anti-virus software offers e-mail protection, I would recommend turning it on. E-mail is still one of the most effective vectors for spreading virii. A good rule of thumb is if you don't know the person, or aren't expecting them to send you an attachment, don't open the attachment. Many virii rely on social engineering to manipulate you into opening their payload.

A person's on-line behavior can determine whether their computer becomes infected with a virus. I would highly recommend against going to any web sites that you wouldn't go to if you were in the office. Off color web sites seem to have more issues with virii than more reputable ones.

2.1.3 Spyware and Adware

According to the Microsoft Encarta College Dictionary, Spyware is "software surreptitiously installed on a hard disk without the user's knowledge that relays encoded information on his or her identity and internet use via an Internet connection."[3] Adware is software that is surreptitiously installed on your computer that shows advertisements in some way shape or form. Spyware or Adware should never be installed on computers that contain sensitive data. Spyware and Adware can slow your computer down drastically. It can also cause it to malfunction to the point where the computer is inoperable. Spyware and Adware can also send personal information to unauthorized parties.

Some seemingly reputable companies will bundle Spyware with their applications. The reason is monetary. They get paid per installation. I would recommend installing some sort of anti-spyware program. Many of the anti-spyware programs are freeware. I would strongly recommend doing some research before installing a solution. Some products are more effective than others. Some unscrupulous vendors will even create false positives to get you to buy their product, so "Caveat Emptor" is the watchword when selecting a product.

Like its anti-virus software cousin, anti-spyware software requires periodic updates to its signature database. If the product offers it, I would recommend turning on its auto-update feature. I would also select a product that offers "real time" protection. This feature will help prevent the Spyware from getting installed on the computer. If the software doesn't work in "real-time," the software is simply cleaning up after the computer has already been infected.

[3] Microsoft Encarta College Dictionary, Page 1399

2.1.4 Operating System & Software Patches

All operating systems and software have flaws. Periodically, fixes are distributed by the software companies to remedy these flaws. The patches need to be done to keep the computer secure and functioning properly. Sometimes the patches can have unintended consequences.

I recently had a server that had been rock stable for three years. Several security patches were issued for its operating system. After the patches were installed, the system was prone to abending multiple times during the day. The patches caused the system to become unstable. Before installing any patches to a computer, it's a good idea to consult with your IT department. They may know if the patches will cause any problems. If you don't have an IT department, it's best to do some research on the patch before applying it.

If problems do occur, the above-mentioned consultation will give the IT staff a clue as to what was done to the computer. If you do something to the computer, be up front with the IT staff. It takes much longer to fix a problem if you don't have all of the necessary information.

2.1.5 Metal Detectors, Magnetic Media and X-ray Machines

Floppy disks, video tapes, back up tapes, audio tapes and any other magnetic media can be damaged by metal detectors and incorrectly configured x-ray machines.

I was recently asked to investigate why some of our employee's floppy diskettes would spontaneously become unreadable. After doing some experimentation I found that 20 percent of the diskettes sent through the lobby x-ray machine would become unreadable. We no longer send any magnetic media through the x-ray machine or magnetometer. It is all hand inspected. Thumb drives, flash memory cards and optical media are immune to this effect.

Most screeners will tell you that their equipment is safe for magnetic media. My recommendation is to insist on them manually inspecting any questionable articles. It's better to be safe than sorry, especially when your presentation is on a floppy disk.

2.1.6 Use Strong Encryption on Removable Media

Things get lost. It's a fact of life. Suppose that floppy diskette containing your complete legal strategy fell out of your briefcase, would you want the person finding it to be able to read it? In most cases the answer would be no.

Strong encryption scrambles the information on the media so that only people with the proper key and/or password can access it. Encryption can be a double-edged sword. If

you forget your password or lose your secret key, the encrypted information will become unrecoverable with the resources that most of us have at our disposal. All encryption is breakable if you have enough time and computer power. Fortunately or unfortunately the only organizations with such resources are usually governments.

Most thumb drives can be purchased in “secure” flavors. Some of these drives have encryption software included on them. Other more elaborate units have biometric authentication built into them. This usually takes the form of fingerprint identification. Before implementing any sort of encryption scheme, you should check with your IT department. There may be corporate or regulatory mandates that preclude its use.

If you can’t use encryption because of a corporate policy or regulatory mandate, you should at least password protect your documents using the utilities included within most word processing, spreadsheet or presentation software programs. Password protection is better than no security on a document. In most cases it will keep the casual observer out.

2.1.7 Off Site Backups

As we saw in section 1.2.6, off site backups are critical. They can literally be the difference between success and failure. The backup scheme does not have to be elaborate. It can be as simple as putting floppy diskettes containing changed documents into a safety deposit box. It can be elaborate as doing nightly tape backups on all of your computers. If you’ve taken the precaution of splitting up your team by having staff stay at different hotels, off site backups become relatively easy. Just give the backup media to staff staying in a different hotel.

Most operating systems come with some form of backup utility. In most cases the included backup utility will be sufficient to backup the workstation. If you are using some other backup solution, you should have a copy of the software installation disks with you. Should a computer need to be rebuilt, the operating system may not have the ability to read backups written in that “other” backup software. Off site backups should also always be encrypted if the backup software supports it.

Periodically you should do a test restore from your backup media. I have seen a few situations where backups were being done nightly but no one ever bothered to see if they could restore from the media. In both situations there were issues with the media that prevented them from restoring.

How often you run backups depends on how valuable your data is. I would recommend doing a full backup nightly. With most backup software packages, once you start the process it runs unattended. Start the backup, then go have a nice relaxing dinner.

2.1.8 Connecting to Evidence Presentation Systems and Remote Monitors

Most modern courtrooms have “Evidence Presentation Systems.” In a nutshell, these consist of a VCR, Document Camera, Audio Tape Player and external computer inputs which interface with the courtroom’s audio system. Another component of the system are computer monitors that are distributed throughout the courtroom which allow viewing of the evidence.

When you connect your computer into an evidence presentation system or remote monitors, you should have some method of disabling the VGA output of your computer that you control. This can be as simple as using <function> F8 to shut off the external VGA output on your laptop or it can be an external switch box between your computer and the Court’s system.

Sometimes the inputs on the Evidence Presentation System will inadvertently get switched on. This is why you need to locally control the VGA output of your computer. It’s a bad thing for the Jury to see you lose at Solitaire. It’s even worse for opposing counsel to see you working on your case notes. I have seen both of these situations happen in open court. The Jury was amused. The attorney that it happened to was not.

2.1.9 Can I Leave This Computer Here?

Computers containing sensitive data should never be left unattended in a courtroom or unsecured area. One obvious problem is physical theft. Things tend to get stolen when they aren’t supervised. A more interesting problem is data theft.

As an experiment for this paper, I attempted to see how fast I could steal data from an unsupervised computer. For the record, all of the computers in this experiment were mine, so no ethical rules were broken or bent.

The following tools were used in my experiment: a Symantec Ghost™ boot disk, a network crossover cable and a laptop with Symantec Ghost™ Server installed on it. The target computer was quite ordinary, a Dell laptop with a floppy disk drive and a 10 gigabyte hard drive. The laptop had an integrated 10/100 network card.

I was able to fully copy a 10 gigabyte hard drive in less than twenty minutes. The victim computer showed no evidence of being tampered with. Once I had an image of the target computer, I was able to extract any file at will using the utilities that come with Symantec Ghost™.

There were some simple changes I could have made to the “victim” computer to impair this attack. If the computer had a BIOS password on it as was discussed in section 2.1.1, the time required to copy the hard disk would have been greatly increased or the attack may have been foiled all together, depending on whether the attacker was able to bypass the

BIOS password. If the floppy drive and CDROM drive had been physically removed from the laptop, I would have had no way to run the necessary software to copy the hard drive. Unfortunately most computers aren't configured this way.

2.1.10 Copiers & Fax Machines

Most modern day copiers are multifunction machines. They have the ability to fax, copy, scan and store documents. With this increase in functionality comes an increase in possible abuse.

Some copiers have the ability to "Demand Reprint." This feature stores a copy of your document on the copier so that it can be reprinted, faxed or e-mailed at a later time. This function makes it simple for an attacker to obtain a copy of your documents. Any time you use an unfamiliar copier, you should make sure this functionality is turned off.

Another function to be concerned about is "Fax Forwarding." This feature allows a fax to be printed then retransmitted to another fax recipient. If the machine has been compromised, it is possible that faxes could be relayed to unauthorized parties. Before faxing anything I would verify that this feature is not turned on.

2.1.11 Hotel Networks

Special precautions should be taken when connecting your computer to the hotel's network or internet connection. Keep in mind, this is not your DSL connection at home. You have no idea who else is on the network with you and whether their computer is free from hostile programs.

Depending upon the architecture of the hotel's network, your data may be observable from each network jack on the network. If the hotel's network is wireless, it is entirely possible for someone to monitor your network traffic using a homemade antenna manufactured from a soup can. A "Cantenna" can have over a mile range.

All computers connecting to unfamiliar networks should be protected by a firewall. The definition of a firewall is:

> *A system designed to prevent unauthorized access to or from a private network. Firewalls can be implemented in both hardware and software, or a combination of both. Firewalls are frequently used to prevent unauthorized Internet users from accessing private networks connected to the Internet, especially intranets. All messages entering or leaving the intranet pass through the firewall, which examines each message and blocks those that do not meet the specified security criteria.* [4]

[4] http://www.webopedia.com/TERM/f/firewall.html

Some firewalls are hardware devices which are installed between your computer and the unfamiliar network. Other firewalls are software programs which are installed on the computer. For general purpose protection either style is sufficient.

When accessing hotel networks you should always assume that you are being monitored. This monitoring can be legitimate, such as the hotel's IT staff monitoring the network's performance. It can also be illicit, like the bored hacker in room 202 scanning network traffic for passwords.

If your company has Virtual Private Network capabilities, you should connect to it before surfing the internet. The VPN will act as an encrypted tunnel between the hotel's network and your corporate network. The encryption will make it difficult if not impossible for someone unauthorized to monitor your activities. If you don't have VPN access, you should avoid using protocols that are not encrypted. A few of the major clear text protocols are: HTTP, FTP, and TELNET.

References

Computer theft hobbles Blake defense, (2 December 2004) URL: http://www-cgi.cnn.com/2004/LAW/12/02/blake.wifeslay.ap (24 January 2005)

How do I reset a BIOS password?, URL: http://corky.net/2600/computers/reset-bios-password.shtml (24 January 2005)

Ward, Mark. “Cyber crime booms in 2004" (29 December 2004) URL: http://news.bbc.co.uk/1/hi/technology/4105007.stm (24 January 2005)

Microsoft Corporation. "Spyware". Microsoft Encarta College Dictionary. 2001 ed

Wienbar, Sharon. “The spyware inferno” (13 August 2004) URL: http://news.com.com/2010-1032-5307831.html (24 January 2005)

Howes, Eric L. “The Spyware Warrior Guide to Anti-Spyware Testing” (2 October 2004) URL: http://spywarewarrior.com/asw-test-guide.htm (24 January 2005)

Howes, Eric L. “Rogue/Suspect Anti-Spyware Products & Web Sites” (20 January 2005) URL: http://www.spywarewarrior.com/rogue_anti-spyware.htm (24 January 2005)

Maxell Data Media FAQ, URL: http://www.maxell.com/Content/Pages/Page.asp?Section=FAQs&Department=datamedia_faq&Line=floppy_faq&Open=xrayfloppyfaq (24 January 2005)

Smith Kevin K. “Do you copy? Security issues with Digital copiers”. (16 September 2000) URL: http://www.giac.org/practical/gsec/Kevin_Smith_GSEC.pdf (24 January 2005)

Garrard, David L. “A Security Assessment of the Ricoh Afcio 450E Multifunction Device” (9 July 2003) URL: http://www.sans.org/rr/whitepapers/networkdevs/1211.php (24 January 2005)

Rehm, Gregory. “How To Build A Tin Can Waveguide WiFi Antenna” (2004) URL: http://www.turnpoint.net/wireless/cantennahowto.html (24 January 2005)

Firewall, URL: http://www.webopedia.com/TERM/f/firewall.html (24 January 2005)