GIAC Security Essentials Certification (GSEC) Practical Assignment
Version 1.4b – Option 1

Title: **Security Awareness for Small and Mid-Size Businesses – Educating the Business Owner or Manager**

Author: Martin E. MacDonald

Date: January 10, 2004

Introduction

Security awareness in Small and mid-size business (SMB) enterprises is relatively low. This is caused by many factors. Smaller businesses generally do not have the resources to commit to specialized information security staff. They also lack the financial resources to implement many types of hardware and software protections such as multiple servers for segregating at-risk assets and intrusion detection systems. There is a prevalent attitude that, because they are a small business, they are an unlikely target for information system security breaches.

Convincing the owner or manager of the need for better security measures and security awareness training is the goal of this article. It attempts to use real life examples to which the owner or manager can relate. By writing in a conversational mode, the end result may be a guide that security assessment personnel can use to convince SMBs to both re-evaluate their security policies and to commit to a program of policy reviews on an annual basis.

[Mr. Johnson (SMB owner)] – Hello.

Hello, Mr. Johnson. I realize that, as president of your retail and distribution business that you are a busy man. I won't take much of your time. I was contacted by your network administrator to talk to you about doing a security assessment of your information systems. Your network administrator believes that you have good security procedures in place, but he also felt that he may be overlooking something important.

I'm calling from Information Security Specialists. We conduct security assessments. I'm confident that we can help you.

Your network administrator says that you are diligent users of antivirus software and that you have a good firewall system in place. Both of these are excellent means of protection for your internal systems from external threats. It's good that you have these in place.

But is antivirus software and a firewall enough? Are there other threats that should be addressed? Most certainly there are! In fact, quite possibly you've overlooked the largest single threat to your system. This is the threat of an insider attack!

Another significant threat you should consider is the fact that your valuable company information is often leaving the protection of your antivirus system and your company firewall and is literally walking out the front door.

[Mr. Johnson] – Why might this happen to my business?

Most Small and mid-size businesses do not have dedicated security professionals on their staff. They rely on internal personnel to run and maintain their information systems and network infrastructure. These employees are often brought into the maintenance task from another discipline, such as from the accounting office, from the engineering office or even from the sales office. The employee is often selected for the task because they show proficiency with computers, or because they are already charged with custody of sensitive information. How can these employees possibly keep abreast of the rapidly changing threats to information security?

Even if the above staff was specifically hired to run and maintain the internal networking system, they were most likely picked because of their knowledge of hardware configurations and network operating systems. Do these people have the requisite knowledge of controls and security measures to keep your valuable company information secure?

Your internal information systems personnel will most likely rely on vendor supplied checklists and standard, out-of-the box configuration guidelines to set up your network configuration, access and password policies. Is this enough to maintain the confidentiality, integrity and availability of essential company resources? Do your employees understand the full nature of the threats confronting their information domains?

Educating both business owners and their employees in charge of maintaining critical information systems is a difficult task for many reasons. The largest hurdle that security professionals must jump is the hurdle of complacency. The most prevalent attitude of small and mid-size business owners is that they are too small to worry about the types of incidents that make the national news.

You have a firewall in place. Because of this, you probably feel protected from outside hackers attempting to penetrate your network. Besides, you are a small business, therefore who would want to hack your system?

You have antivirus software in use. This protects you from problems with e-mail related threats. Your network administrator keeps the virus definitions up-to-date. This is a good policy and has likely saved you from the loss of productive time. It probably stops many virus attacks on a daily basis. Why should you worry about anything more?

Let's talk about the two threats have not been addressed. Specifically, let's talk about the threat of an insider attack and the threat to valuable company information leaving the protection of your firewall and antivirus system.

[Mr. Johnson] – What do you mean by an Insider Attack?

Insider attacks take many forms. They include theft of company assets. These include both physical assets and information assets. Another form of insider attack is due to malicious acts by disgruntled employees. Many small and mid-size business owners feel that they have trustworthy employees. You may feel this way about your employees. You don't have to worry about this threat. Or do you?

According to the 2003 CSI/FBI Computer Crime and Security Survey compiled by Robert Richardson, 56% of the survey respondents had detected unauthorized use of their computer systems in the past year and commented that "…theft of proprietary information caused the greatest financial loss…" of all types of breaches of 530 companies surveyed.[1]

Over a third of the companies surveyed had less than 500 employees. In other words, they were very similar to your company.

Computer theft is also a serious problem, particularly, theft of mobile computers. In fact, many of these thefts occur right from within your company offices. A growing problem for businesses is the theft of laptops and personal digital assistants (PDAs) by *office creepers*. These are neatly dressed thieves who will enter an office with the goal of walking off with company computers. How can such thieves get away with this crime? It is caused primarily by lack of security awareness by company employees. According to Mark Niesse, "Office creepers have legions of unwitting accomplices – employees with a false sense of security."[2]

You indicated that you trust your employees. I'm hopeful that they won't steal from you. However, dishonest and disgruntled employees are not necessarily seeking personal gains. While some may be stealing information for their own profit and some may be stealing physical assets for themselves, others may simply be trying to punish or get back at their employer or their supervisor for perceived wrongs.

A disgruntled employee can do harm to you by deliberate sabotage of company records. This can be done through deletion of critical records. It can be done by deliberately recording invalid or fictitious data. Both of these types of malicious acts are usually easily traceable to the employee, based on their user login. Consequently this type of misuse is avoidable by employing proper access controls and through internal controls that validate information that is entered.

Most employees know or suspect that such controls are in place so they are unlikely to perform malicious acts that are so easily traced. Instead, they prefer the anonymity of releasing information to third parties and simply watching the results of their actions.

Examples of this type of malicious attack hit the news daily. Many well known companies are victimized. In a recent incident reported by Associated Press, an American Eagle Outfitters employee was caught for his actions.

> Federal prosecutors said that Patterson posted user names and passwords for American Eagle users on an Internet hackers' group bulletin board and detailed instructions on how to hack into the company's system after he was fired last year.[3]

And yet another incident of malicious spite from a recent headline reported in Computer Security News involved a New Zealand based ISP. The fact may be that this individual did not intend harm. However, once confidential items are released to the Internet, they are there forever. “The Herald says that the apparent owner of the site, a 14-year-old who used to work for Net4u, told the paper that he admitted posting the information, but now regretted the matter.”[4]

Another form of insider attack is one where your employees are unsuspecting accomplices. This is where an employee reveals or divulges valuable company information without realizing what they have done. Your employees may reveal this information when someone from outside the company uses social engineering techniques on them.

What is social engineering? Social engineering is hacker-speak for tricking a person into revealing something about their internal security that should not be revealed. Social engineering is a con game. The Whatis.TechTarget.Com web site offers a detailed definition of social engineering.

Why is social engineering a danger to businesses? It comes down to the value of company information. The company has it and the villain wants it.

Specifically, "Social engineers rely on the fact that people are not aware of the value of the information they possess and are careless about protecting it."[5]

What are examples of social engineering? Examples can be a simple as *shoulder-surfing*. This is where someone tries to get another users password by watching over their shoulder as they log in.

A more complex scam may be the phone call to your help desk or receptionist where the caller has some information about one of your users or employees and tries to trick the help desk employee or your receptionist to reveal the missing information. In fact, there are hacker training materials available that instruct would-be hackers on exactly how to do this.

An example of such instructional material is contained in the Summer 2003 issue of 2600 magazine.

> …many people do not realize just how easy it is to obtain information and use it. Personal information such as your name, phone number, and address can be obtained as easily as making a phone call to a utility company such as your local electric or phone company. In this article I will run by a few social engineers I have used in the past that have proven to be reliable time and time again (Lucky225, p.14).[6]

Finally, another type of social engineer is a more elaborate scam that involves posting very legitimate looking information on a web site and then getting your employees to reveal information about themselves or about your company on the web site.

A recent example of this is the Citibank fake e-mail scam as reported by Linda Rosecrance in PCWorld.com.[7] In this scam, customers of the bank were sent a fake e-mail with a link to the scammer's web site. The e-mail contains enough valid information to make the reader think it is legitimate. On the fake web site, the scammer asks the user to provide their user name and password to log in to the bank site, thereby capturing the user's information for the hacker's use.

While social engineering is not exactly defined as an insider attack, the results can be much the same as from lack of adequate physical protection of critical information assets.

[Mr. Johnson] – You also mentioned my information leaving the protection of my firewall and antivirus software. How might this happen?

How mobile are your employees? If you send employees on business trips with company computers, then you should be asking “How mobile is my company information?”

Mobile computing is becoming a normal mode of operation for employees of many companies. With the implementation of wireless networking (also called Wi-Fi technology) this trend will accelerate. This means that employees are taking company assets outside of the protection of the company firewall. In many cases, it also means that the antivirus protection on the mobile computer is not as up-to-date as it is on always-connected computers.

Company assets not only include the computer but also the sometimes irreplaceable company information contained on the computer.

There are many threats to users of mobile computers. As mentioned above in the section on office creepers, laptop computers and PDAs are favorite targets of theft within the company. It should then be no surprise that they are also a target of theft outside of the company.

Brigadoon Software, Inc recently conducted a survey (2003 BSI Computer Theft Survey)[8] to accumulate data on business vulnerabilities to computer theft. The survey had 676 participants from throughout the world, from all size businesses. According to the survey, 44.5% of the participants had been the victim of a computer theft in the last 12 months. Of the total thefts, 48% were laptop computers and 13.3% were PDAs. Again of the total thefts, 53% occurred while the computers were mobile.

Most business can suffer the loss of the computer equipment. But what about the information that was on the computer? This is, by far, the more important issue. While two-thirds of the participants placed the value on the stolen computers at $25,000 or less, 9.2% of the respondents estimated the value of the stolen information at over $1 Million.

How valuable is your company’s information? How valuable is information about your company that is stored on another business’ computers? Even our government has a problem in this area. Declan McCullagh of Wired News reports:

> Treasury Department auditors did not give very high marks to the IRS in this regard. “Losing your laptop may be a major headache for most people, but for America’s tax collectors it happens all the time. The IRS has lost or misplaced 2,332 laptop computers, desktop computers and servers over three years.[9]

Your company firewall provides no protection if the computer itself is stolen. Furthermore, your employees may be connecting the laptop to unprotected networks while on their business trips. These networks take many forms. One example is the network inside the hotel at which the employee is staying. Another example is the hot spot at the local coffee shop. Your company's firewall provides no protection in this instance.

What about your antivirus software. Well, it's likely that your laptops are protected from viruses even when their not connected to the network. However, how current is the virus definitions file? Your network administrator is updating the definitions file on a daily basis at your office, but this does little to protect the laptop user while on their business trip. What could the laptop user be doing to protect themselves?

Finally, have you even considered the possibility that your employee's PDA may be subject to attack? Personal Digital Assistants are no longer the simple electronic calendar and address book they used to be. Many are now full-fledged mobile computers. As such, they need the same protections as a laptop computer.

[Mr. Johnson] – O.K., you've got me interested in information security. What should I be doing?

Well, Mr. Johnson, I'm sure that you understand the principles of physical security. Undoubtedly, you have locks on your office and warehouse doors. You probably issue master keys to only certain select employees. You're likely to have fire-sprinkler systems and smoke detectors in your buildings. These help to protect physical assets in emergency situations.

You must understand that the goal of information systems security is to protect your most valuable company asset, your company's private information. However, these goals extend beyond the simple protection of information.

The goal of information security is often referred to as the objectives of C-I-A. This stands for Confidentiality, Integrity and Availability. That is to say, you want to maintain the confidentiality of the records, you want to be assured that the records maintain their integrity, and those records need to be available as needed in your business.

As you can see, in certain situations, a trade-off must be made. For example, you may have to loosen controls in one area to balance the availability of the information with the controls you might put on the records to maintain their confidentiality.

You have already taken steps to maintain the confidentiality of information by implementing a company firewall. This protects your internal network and the information on it from unauthorized access by outsiders.

You have also taken steps to maintain the integrity of information by implementing antivirus software. This helps to protect your information from being altered by malicious code introduced from the outside.

Where you may be susceptible is that you may have made your information too easily available to employees within your business. This is what makes you vulnerable to possible insider attacks.

Another concept that we use in information security is the concept of Defense in Depth. This concept is quite simple. It means that you don't rely on only one means of protection. Instead, if the primary means fails, you have a secondary backup system in place behind the primary one. Furthermore, you will want a tertiary system to back up the secondary one. In other words, you use as many layers of protection as economically feasible to assure the confidentiality, integrity and availability of your important information.

Perhaps an example will help to illustrate what I mean. I mentioned earlier that you probably have a fire-sprinkler system in your offices. But is this all you have? I suspect you have more.

For example, you probably don't allow employees to start fires in the first place. You may have a policy of no personal heaters or coffee pots at the employee's desks. You may have a designated kitchen area or a designated area for smokers. Both of these measures are a first line of defense and are based on policies. Secondly, you probably have fire extinguishers in selected areas of the office. This is a second line of defense in that it helps to extinguish small fires once detected by your employees. As a third measure of defense, you may have an automatic fire-sprinkler system. This protects the building itself, as well as the safety of your employees if the fire is beyond the capabilities of your employees to extinguish, or if the fire occurs when no employees are present. Next, you're likely to be in a community with a fire department. This line of defense assists you in protecting the lives of your employees and your assets beyond the control of your fire-sprinkler system. Finally, you probably have fire insurance coverage as part of your commercial liability insurance package. This helps to protect the continuation of your business if you are unable to preserve the value of the assets.

As you can see from the above example, you already have many layers of defense to protect you from the threat of fire. The concept is the same for your information system assets. You need to evaluate the threat to which these assets are exposed, and then devise as many layers of protection (Defense in Depth) as is economically viable for your business.

Let’s now talk specifically about the two threats we discussed earlier. Those threats were the threat of an insider attack and the threat due to the loss of computers and PDAs.

Protecting Against Insider Attack

One of the first means of protection from insider attack is the simple protection of access control. I assume that you are using passwords when users log on to the network. This is standard practice. If your network administrator followed the operating system guidelines, he’s likely to have instituted this measure.

However, this may not be enough. Another guideline to be followed, but one that’s often overlooked is the principle of least privilege. In other words, you should give each employee access to the least amount of information they need to do their job…*and no more!*

The principle of least privilege means that an employee could not make unauthorized forays into areas of your network that they don’t have a need to know.

Again, you are likely to have done some of this already. For example, your warehouse employees probably have no access to your accounting office records. Likewise, you probably restrict your personnel records to your human resources manager. These are both examples of the principle of least privilege at work.

As we discussed previously, attacks by means of social engineering can be the most effective. To specifically combat such attacks, you must examine the vulnerabilities and protect your company by all means that are economically feasible.

Social engineering attacks can best be prevented by early detection. Because this type of attack is against your people, the best way to prevent the attack is through the implementation of security policies while the best way to detect the attack is through staff awareness training.

Examples of security policies go beyond the implementation of user names and passwords. They extend into the area of operational policies as well as computer access policies. For example, you may want to institute a policy of shredding documents prior to disposal. This protects against the “dumpster diving” attack for sensitive information. You might install locking doors between your administrative offices and your warehouse storage room. This protects confidential information from shoulder surfing types of attack by employees not normally privileged to be in the administrative offices.

Of course it's better to detect an attack before it reaches the prevention measures. Security awareness training is the best method to enable to your employees to recognize the tactics used by people hackers. Educating all employees is critical. While it's true that your support staff is the most likely targets of such hackers, it's important all employees be given the education to recognize the types of possible scams.

Your support staff might be asked to give out passwords, PIN numbers, account numbers, and other such information. They should absolutely refuse to provide information without proper authorization. While the person on the phone may be proclaiming the need for the information, your customers will appreciate the fact that you refuse to disclose information without first verifying the security level of the caller.

There are many means available to educate your staff about social engineering. This can be done through annual classes, through employee newsletters and by warnings placed on signs, mugs, posters and screensavers. The important part of the process is to constantly remind your staff as to the importance of security and, through proper security, the benefits to your company and, by extension, to their own employment. This will give the employees a sense of responsibility for the security of the information.

A good primer on methods to use to spot social engineering attacks is an article written by Sarah Granger published on the web site of the Computer Crime Research Center (CCRC). In this article, she indicates that in order to foil an attack, one must be able to recognize one.

> The Computer Security Institute notes several signs of social engineering attacks to recognize: refusal to give contact information, rushing, name-dropping, intimidation, small mistakes (misspellings, misnomers, odd questions), and requesting forbidden information. "Look for things that don't quite add up." Try thinking like a hacker. Bernz recommends that people familiarize themselves with works such as Sherlock Holmes stories, How to Make Friends and Influence People, psychology books, and even Seinfeld (he and George Costanza do have a knack for making-up stories)[10]

As you can see, protection from social engineering attacks or people hacking attacks is an on-going, never ending process. One of our goals at Information Security Specialists is to provide businesses with a means to keep abreast of such matters and to schedule regular sessions of security awareness training for businesses.

Protect Mobile Information

I hope that you now recognize the fact that valuable company information often leaves the shield of your company's firewall and antivirus software protections through the use of mobile computers and PDAs. Let's talk about a few specific measures you can take to better protect this information.

I suspect that when your users connect their laptop computer to the company's network, they are required to use a user name and login, the same as if they used a desktop, always connected computer. The user name and password provide two valuable pieces of information to your network. It provides information as to whom they are (user name) and something only that user should know (password).

These are two aspects of access control techniques used on trusted computers. That is, because the computer is located behind your own company's firewall, you have a high confidence level (trust) that the user has the right to use and store the information on the local machine. Once information is accessed, a significant amount of information is stored on the local hard disk of the computer in the form of temporary files, swap files, cache files, history files, etc.

How might this be better protected on a laptop or mobile computer? One method would be to add an additional component to the access control policies. A common way to do this is to add something the user has, to something the user is (user name) and something the user knows (password). The most common access control methods based on something the user has are biometric devices and smart cards. These are particularly effective if they are required for boot-level access to the mobile computer.

In this instance, if the mobile computer is lost or stolen and if a hacker were able to crack the user's name and password, the hacker would not be able to boot it, or remotely connect it to the company's network without the access control device. This may protect the company from a hacker's use of the missing computer, but what about the information already on the mobile computer's hard drive?

An additional protection that might be used is an operating system that encrypts the data stored on the hard drive. For example, Windows operating systems newer than Windows NT provide an Encrypting File System. The value of this is that it can protect the data on the mobile computer hard drive. Therefore, if a laptop or mobile computer goes missing, and even if the hacker pulls the hard drive and moves it to another laptop computer in order to get around the boot-level password protections, the hacker will still be unable to read any information stored on the hard drive without the decryption key.

You've now seen how we might protect your network from a hacker's unauthorized use of a company-owned mobile computer and how you might protect the company information stored on mobile computer itself. There is another threat to discuss and that is the hijacking of a mobile user's wireless communications signals.

Standard wireless communications rely on an encryption technology called Wired Equivalent Privacy (WEP). However, given enough time, a determined hacker can break this encryption scheme. In order to raise the bar for hackers to jump over, you should utilize end-to-end encryption at the higher network protocol layers. This means using solutions such as Secure Shell (SSH), Secure Sockets Layer (SSL) or true Virtual Private Networking (VPN) for making your session connections. In other words, don't rely on out-of-the-box configuration settings for your company's protection. Instead, raise the level of protection to the highest standard available, keeping in mind a reasonable cost.

You should also pay attention to your antivirus policies for the mobile computers. While your networked computers are getting a daily checkup, assuming you are downloading virus definitions daily, your mobile computers may need a different configuration.

You may want to configure both your laptop computers and your PDAs with stand-alone antivirus software. This software can then be configured to check for virus definitions daily, whether or not the computer is connected to your network. In this manner, the mobile computer is protected even though it's on the road with your employees. This may seem like a bit of an inconvenience for the mobile employees. However, ask your employees how inconvenient it would be for them to lose the use of their computer while on the road, particularly if they are about to make an important sales presentation.

There are several vendors now making antivirus software with laptop and handheld computers in mind. Many of these can be managed as stand-alone applications on each machine, or managed through an enterprise wide solution.

[Mr. Johnson] – I had no idea that my staff and computers were so vulnerable. How do I start a better program?

That's where we can help. At Information Security Specialists, we provide many levels of service. The starting point is a basic security assessment. This is a program whereby we review your existing policies, configurations and usage of information technology and then report to you our general observations.

It's important to emphasize that our job is not to criticize your existing information systems personnel. Our goal is to help you better protect your company. Please recall that it's extremely difficult for your internal staff to stay abreast of all the possible threats and vulnerabilities in your systems. They are likely busy with their daily tasks of offering support to your other users, dealing with daily backup routines and the ubiquitous spam problem.

In fact, you should be aware that many businesses are now required to certify that their internal control systems are adequate to detect and prevent fraud within their companies. Currently these rules only apply to publicly traded companies. They are imposed by the Sarbanes-Oxley Act of 2002. However, we expect the banking industry to begin adopting these standards for businesses to whom they loan funds. This will go beyond publicly traded companies, perhaps even to companies such as yours.

In a recent whitepaper, issued by Guidance Software, Inc., John Patzakis and Victor Limongelli had this to say:

> According to Greg Schaffer, Director of Cybercrime Prevention and Reponse for PriceWaterhouseCoopers, Sarbanes-Oxley's requirements "are causing many public companies to hire investigators, including computer forensic experts, far more regularly to review allegations of wrongdoing or indications of potential fraudulent activity detected by internal company control structures."[11]

Because of the effects of recent legislation such as the Sarbanes-Oxley Act of 2002, the Gramm-Leach-Bliley Act of 1999, and the Health Insurance Portability and Accountability Act of 1996, we recommend that companies institute a program of annual reviews of their information security systems by credentialed professionals. This offers a level of assurance and accountability that you may otherwise not be able to reach using internal employees.

We offer this service as a follow-up to our initial security assessment program. In other words, we'll be able to review policy changes that you implement, new threats or vulnerabilities that arise due to changes in technology and the effect of changes in configuration or expansion of your information systems. We recommend that this be done at least annually.

[Mr. Johnson] – O.K. I'm convinced. When can you start?

Reference:

[1] Richardson, Robert (Editorial Director). 2003 CSI/FBI Computer Crime and Security Survey. San Francisco, CA: Computer Security Institute 2003. 4.

[2] Niesse, Mark. "Upscale thieves steal laptops, PDAs in offices." Mercury News 28 November 2003. URL: http://www.siliconvalley.com/mld/siliconvalley/7369019.htm?template=contentModules/printstory.jsp

(3 Jan 2004)

[3] APOnline via COMTEX. “Man Sentenced for Hacking Into Web Site”. Pittsburgh: Associated Press 3 December 2003, URL: http://www.prophet.net/quotes/stocknews.jsp?symbol=AEOS&article=337w6703 (3 Jan 2004)

[4] “NZ Hacker Places ISP Customer Details on Web”. Computer Security News 18 September 2003. URL: http://www.infosecnews.com/sgold/news/2003/09/18_06.htm (3 Jan 2004)

[5] “social engineering”. searchSecurity.com Definitions 05 April 2001. URL: http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci531120,00.html (3 Jan 2004)

[6] Lucky225. “Staying Anonymous in the Information Age”. 2600 The Hacker Quarterly Summer 2003, Volume Twenty, Number Two. 14.

[7] Rosencrance, Linda. “Citibank Customers Hit With E-mail Scam”. Computerworld 27 October 2003, URL: http://www.pcworld.com/news/article/0,aid,113118,00.asp (12 Dec 2003)

[8] Source 2003 BSI Computer Theft Survey (www.BrigadoonSoftware.com) :Executive Summary iii – Pages 1-2.

[9] McCullagh, Declan. “IRS’ Case of the Missing Laptops”. Wired News 10 January 2002. URL: http://www.wired.com/news/politics/0,1283,49615,00.html (3 Jan 2004)

[10] Granger, Sarah. “Social Engineering Fundamentals, Part II: Combat Strategies”. Computer Crime Research Center, URL: http://www.crime-research.org/eng/library/Razum2.htm (3 Jan 2004)

[11] Patzakis, John and Victor Limongelli. “Internal Computer Investigations as a Critical Control Activity Under Sarbanes-Oxley”. Pasadena, California: Guidance Software October 2003. p. 3