Global Information Assurance Certification Paper

David McGuire

GSEC Practical Assignment Version 1.2d

Controlling Inside Threats: Stalking the Wild End User

Introduction

Threats come to a computer system from two sources: those outside the firewall, and those inside the firewall. Outside threats are often more dramatic than inside threats - the cola crazed hacker breaching the firewall at 3 AM is a popular stereotype. However, inside threats will occur more often and consume more of a Security Manager's time. As well, outside attacks often succeed because an inside threat wasn't managed properly.

It's an information jungle out there and your end users are the denizens of the jungle. It's up to the security manager to tag and tame them. You can't policy security problems away easily, because employees must co-operate with security policy to keep an environment secure.

If you don't think inside users are a threat, go cruise around the flirt rooms on IRC for awhile and see how many people are on from work (the music rooms are popular, too). Is this a security risk or what? If you aren't aware of IRC you are in trouble (for example, 70% of pornography downloads occur from 9 to 5). Go here for a starter course. http://www.irc.org/

End Users and the Inside Threat

Who are the end users? They come in different sizes and shapes. It doesn't matter if they are the CEO, the Accountant, the Receptionist or the IT guy. They are better known by their behavior towards the computer system than by their job function, and so we need a system of classification for them. Then we can develop a plan to deal with them: each according to their abilities, each according to their needs, to borrow from another very old IT guy. But - remember these types aren't mutually exclusive. One day a user can be one type, and another type on a different day. We are dealing with types, not individuals.

A Murder of Crows, A Gang of Wolves, A Gaggle of Geese, A Rout of End Users

Anything that can happen to a computer system can happen from the inside. Who should we be looking for? Knowing an end user's style will help to minimize the risk they cause and put appropriate precautions in place.

1.The break and enter badger:

There are two kinds of thieves: those that are unknown to the organization and those that work for the organization. Right now, I am only concerned with the trusted employee.

Sometimes the theft is minor - a few floppies, a book, an old modem. Sometimes it can be more serious - an expensive software program, a hard drive, RAM, or even a computer.

There are three ways to deal with the thief. First everything has to be locked up- a royal pain but there is no alternative. If you can lock off the entire computer area, so much the better. In smaller organizations this is sometimes impossible - it interferes with friendliness (sometimes friendliness is important to productivity). Also, you really can't lock up the user work areas. You absolutely must lock up the server areas, the laptops, the parts, and the software. This is so much cheaper than the alternative. Secondly, you have to have an inventory. This also is such a pain, but again there is no choice. Whether you do it yourself on a spreadsheet, design a database, or get a commercial program doesn't matter. Confusion will defeat the best laid plan if an inventory isn't written down and updated. Hire a staff to do this if you must, but it must be done. Finally, you need a sign out program. Whenever equipment or software leaves the office, know where it is. This lets the potential thief know you are watching. You can't stop the thief, but this will help.

2. The borrowing budgie:

Closely related to the thief is the borrower. Their insidious behavior will drive you insane. Users want to borrow books, software, computers, modems you name it. Usually you will have some kind of personal relationship with them, or they will have some kind of political power in the organization. Beware of lines like "Is it OK if I take this home to see what it's like?" - so you can approve the theft of the software. They will ask to take something home and then forget to return it. "Just say no?" That isn't always easy or practical. Try to say no. Either you forbid borrowing by policy (don't forget friendliness!) or you make them sign it out. Sometimes it's politically wise to let someone borrow something. Just write it down. Remember to check software for viruses on its return.

3. The clumsy carp:

"Oh oops." In comes a call for help. The dongle on the laptop's Ethernet card gets slammed in a desk drawer. Someone bends the laptop screen back too far. They drop a monitor. They drop a CPU. They trip over a wire and unplug a network. They leave the door unlocked to a secure area. They break things. They delete an important file. These well-intentioned troublemakers can keep you far busier than you might think.

What can you do? Keep the wires untangled. Keep stuff off of the floor. Put things away. Try to encourage everyone to keep their work areas clean. Do good backups. It takes time but this is the only defense. This isn't very glamorous, but it is good security.

4. The rambling roadrunner:

These are the users that work out of the office. They are a nightmare in the making. Off they go with their laptop. They leave it in their car. Or they work from home on an unsecured cable connection. I don't need to list the precautions here - there's too many, but there is main one: get all the rules for out of office written down as a management approved policy and force the roadrunner to sign it. Try to convince the out of office user to at least take a basic computer skills course - better still, a basic security course.

5. The family flamingo:

This person is close related to the roadrunner, but with a few very sensitive twists. This person works from home but shares the computer with the family. They don't believe the family would ever look at the computer, and especially they wouldn't hurt the company data that is on it. Family access to company computers should be explicitly covered in the policy for the out of office user. Try telling someone their kid is trouble with no policy to back you up. If an employee is connected from home, then they must sign a document that shows the computer is secured and that the family stays away from the computer.

Twist one: the roadrunner lends the company laptop to a child doing research at the school library.

Twist two: the flamingo brings the kids along with them to the office when they are working after hours or on the weekend. This should be dealt with in policy! People believe their children are appreciated everywhere.

Twist three: pets at the office? I don't think so (Even though my dog wouldn't be a problem).

Twist four: the child is a computer genius and gives mom or dad a new program that will improve their life. Perhaps the child will change the configuration of the laptop or the home computer so it will 'work better'. This is, of course, accepted unquestioningly by the parent. The kid clearly knows more than you do.

Twist five: did I say child? You can also substitute boyfriend, husband, wife, or any other relative. Add friends, neighbors, and sales people from Future Shop. The list goes on and on.

6. The political pelican:

What is a politician? Well an elected official of course, but at work these people create problems by trying to manipulate organized IT functions. They try to get their jobs done before other users, or their equipment fixed ahead of schedule. This causes problems because regularly scheduled or planned activities get pushed to the side. If the regular activities are important to security, then a risk occurs. These people are often high up in the organization and aren't used to being told "no". There are clear benefits politically to doing favors for them. You have to weigh that risk. Politicians can be controlled by scheduling all activities into carefully defined projects, to-do lists, and prioritized request for service queues. It is a good idea to have these lists available on an Intranet so that everyone can see when somebody gets to line jump. Have a policy rule so only the boss can change your schedule.

7. The powerful peregrine:

Here is a scary user. They know enough to be dangerous, but not enough to be safe. They can disable security programs such as virus checkers or encryption programs. They know how to set up FTP sites and connect to their home Internet accounts from work, or conversely dial into work from home. It's easy to run a sniffer on the network - they can figure this on in a few hours if they want. They don't seem to understand their cleverness can bring the network down. Monitor your network for suspicious activities - run a sniffer yourself, look for promiscuous Ethernet cards. Get your policy set up to allow for standardized desktops and check people who seem to know more often. War dial your network to see if there are any unauthorized modems picking up. Walk around and say hi to everyone once in awhile.

These people are also unafraid to experiment. They will run programs and commands just to see what happens. A strong desktop policy is a help here. State clearly what users are allowed to have. Look for games on the workstations. Have your policy define what users can do. These users are probably the most dangerous people you will have to deal with, and will consume more of your time than anyone else. Policy accordingly.

8. The disgruntled gruntle:

Unhappy employees can deliberately sabotage computer systems. Make sure that you are the first notified when someone is being fired or being disciplined. If someone is resigning, disable thveir privileges as soon as possible. Remove all login rights. Change passwords, locks and phone numbers, depending on the access the user had. The sooner the better. It is important that the other managers discuss with you employees that may have grievances. Monitor those employees more closely if you are suspicious - check their privileges.

9. The scared skink:

This person is the user who only knows enough about their computer to do their job, and sometimes not that much. Unlike the power user, they are afraid to explore their menus. They are also the one most likely to open an email virus. They get their desktops so messed up it takes a boy scout to undo the tangle. They sticky tab their passwords to their monitor. These users have to be trained. Once you spot someone like this, don't rest until they know more. Always talk training for users - it can be as good as a firewall. Get it built into the budget. Training is a good investment for the company.

10. The IT triceratops:

These guys aren't dangerous because they're old or extinct, but because they know too much and have too much power. Goes with the territory, I guess. What can they do? Everything, and cover their tracks as well. Plus you can't watch too hard with out destroying the morale and the strength of the IT department. Your best bet is to play nice with your staff and hope they tell you what they're doing. Make sure they know the dangers of what they're up to. Be generous with them. Try to get IT perks like cheap or free hardware and software, or line time. Get

them active with IT groups so they talk about what they are doing. Meet with them regularly. Keep them busy, keep them happy. Get them interested in security. Your best hope is to make them loyal.

The Roundup

OK. Now you have your groups. How does this change your approach?

The traditional approach to developing a security policy is for the IT department to write one, often in response to some outside pressure on management, then send it up to management for approval, and then down to the users for signing. This is not a bad methodology. Policy resulting from this methodology is a good way to stop outside threats, and control some inside problems. William Farnsworth gives an excellent example of an IT written security policy in his article 'What Do I Put In A Security Policy' (http://www.sans.org/infosecFAQ/policy/policy.htm). However, remembering that most of your time will be taken up with inside threats, it is prudent to start with your users before you write your policy. Forget your users and you will not have a safe system. So, get the users write it (with IT guidance), then to management, then back to the users.

How do you guide them? Be aware that the nature of your users will affect the types of policies and procedures you apply regularly to your users, the effectiveness of your policy, and the way you create your policy. Use these following points as guidelines for your users that are writing the manual.

Regular Precautions

These are security measures that you apply on a daily basis, sometimes without even thinking about it. These include the procedures I have listed under each type of user. They are common sense things that sometimes seem so minor that they don't always make it into a policy or procedure manual, although they should. Lock up your equipment, keep areas tidy, leave the servers locked, don't leave backup tapes on somebody's desk, make sure there isn't water near computers (overhead pipes and coffee cups), don't turn off the virus scanning software, standardize desktops, have fire drills, change passwords regularly, keep an inventory, track help calls - things that we all know but get too busy to monitor. But you had better do it now - it's going to take time sooner or later. Make a checklist based on the types of users you have and go through it. You can focus certain precautions on certain users. If you have a lot of inexperienced users, then training and backup becomes more important. If you have a lot of experienced people, then scanning and lock up may become a priority. If some users handle highly confidential documents then they should use file encryption, and so on. This checklist would vary widely from company to company and be part of the main security policy.

Policy Effectiveness:

OK, here are the rules: 1. Keep your policy simple 2. Get the users to help write it, if not actually do the draft.

Your policy is only as successful as your users choose to make it. You can threaten them, beg them, lecture them, but ultimately your security will stand or fall on user compliance. If they see security policy as one more burden placed on them by management, you can count on stolen laptops (complete with sensitive information on them), hacked modems, and data loss or theft. Your security policy is your most important tool to protect your system - don't let the users ruin the best laid plans.

In order for your users to support your security policy they have to know about it, believe in it, and think that the inconvenience it imposes balances the risk they perceive in the wild. The only way to do this is to maximize the involvement of the users in the creation of the policy. They won't come up with everything on their own, you must be their guide, but they must be involved in every step.

User Involvement

Remember the rules? The users will write the security policy. Yes you are the expert. You will have to be the guide.

Start by reviewing your users. Michele Crab-Guel is one of the few authors identifying this issue. See what she says in her excellent article on writing policy (http://www.sans.org/newlook/resources/policies/bssi3/index.htm chapters 9 and 10 'The Policy Design Process'). How well do you know your users? If not that well, perhaps you should spend some time getting a little familiar with them. Then, get a user group going to write the manual. Start with upper management and tell them what you want to do. Try and get a perk or two for the volunteers - anything, even knowledge is worth something to them. Canvass the users. Chances are, many people will be happy to work on this project - especially if you can do it during work time - real time or virtual chat, matters not. Virtual is kind of fun - set up an IRC server on your network, that's pretty easy. Up to you - this introduces them to some of the fun IRC software and the big world of IRC (another security risk). Then send them some required reading. Here are some examples from TechRepublic. This is a site which deals with all manner of IT things and has some good stuff. This article contains three examples of employee Internet use policy: http://www.techrepublic.com/article.jhtml?src=search&id=r00520000607bal01.htm

Don't use templates as your policy - give the templates to your user committee for background. It's pretty heavy reading. The first example (The Gerontology Network) is through and a little legalistic. The last example (Hurley Consulting) is a little brief. If you have trouble reading this article, think about your users. If you have a security policy that is painful to read, they won't read it. So keep it simple.

One more thing to remember. Keep it readable. It may not be as legalistic if it is readable, but if they don't read it because it's too confusing, you might as well not bother. Stephen Northcott makes a special point of this in his SANS article on writing policy in general (http://www.sans.org/y2k/sec_policy.htm#1).

And don't think it's readable because you made your way through it. Read it out loud to yourself. Have someone who knows nothing about computers read it. See if they understand it. Better yet, have your boss read it. If the boss understands it, anyone can.

Here are some issues to research when you are guiding. Assign a staff to report back on each one of them. Many of these issues are covered in the references below.

1. Legal Issues
2. Training Issues
3. Examples of Security Policy
4. Monitoring network for personal use
5. Staff use of hardware/software/network for personal use

Here are some things to help keep your user group involved. It is easy for them to fall by the wayside. You don't want to end up writing this yourself. Also, a happy member of a user group will be a more productive employee - management may like that.

1. Start a computer group that is relevant to the hardware or software that your company uses.. There are many examples to follow. Look at the local Linux or Mac groups for an example of a user group. Have speakers, have cookies, have it at lunchtime, try to have it meet during work hours.
2. Try to get user training made a high priority for upper management. If it is presented as a security issue, it can make things easier.
3. Set up a shareware lending library for the user group as a reward.
4. Set up an internal chat room or bulletin board so users can touch base. Make sure someone is there all the time to talk to people.
5. Try to get one of your suppliers to give discounts on equipment to members of your user group.
6. Have a reward contest of some kind for the members of your group. This keeps people motivated.

CONCLUSION

A security policy is absolutely essential to control threats to a computer system. Most threats to the system will occur as a result of inside breakdowns. If you have the help of your users, your system will be many times more secure than if the users don't care or are passively/actively resisting you.

Learn who your users are and get them involved in developing a security policy for your organization. Your knowledge of your users will allow you to guide them into writing a security policy that will protect your data.

REFERENCES

Writing Policy:

1. Northcott, Stephen. "Security Policy Research Project". 1999-2000. URL: http://www.sans.org/y2k/sec_policy.htm#1 (May 23, 2001).

2. Hernandez, Ernest D. "Network Security Policy – A Manger's Perspective". November 22, 2000. URL: http://www.sans.org/infosecFAQ/policy/netsec_policy.htm (May 23, 2001).

3. Crabb-Guel, Michele. "Section Three: Policies and Procedures". 1999-2000. URL: http://www.sans.org/newlook/resources/policies/bssi3/index.htm (May 23, 2001).

4. Farnsworth, William. "What Do I Put In A Security Policy". August 10, 2000. URL: http://www.sans.org/infosecFAQ/policy/policy.htm (May 23, 2001).

Examples of Acceptable Use Policies

5. U.S Department of the Interior. "Internet Acceptable Use Policy". May 23, 1997. URL: http://www.doi.gov/footer/doi_aup.html (May 23, 2001).

6. EFA. "Model Acceptable Use Policy for Employee Use of the Internet". November 20, 2000. URL: http://www.efa.org.au/Publish/aup.html (May 23, 2001).

7. Baldwin, Paul. "Samples of Acceptable Use Policy". June 7, 2000. URL: http://www.techrepublic.com/article.jhtml?src=search&id=r00520000607bal01.htm (May 23, 2001).

8. TechRepublic. "A Framework for Internet and Email Use Policies". January 1, 2001. URL: http://www.techrepublic.com/download_item.jhtml?src=search&id=dr00520000606bal01.htm (May 23, 2001).

The Employees Perspective

9. Vault.com. "Samples of Internet Use Policey". January 2, 2001. URL: http://www.vault.com/surveys/internetuse2000/index2000.jsp (May 23, 2001).

10. Vault.com. "Survey Results of Internet Policies. January 2, 2001. URL: http://www.vault.com/surveys/email_behavior/email_behavior.jsp (May 23, 2001).

11. Baldwin, Paul. "TechRepublic Members Sound Off On Internet Use in the

Workplace". June 19, 2000. URL: http://www.techrepublic.com/article.jhtml?src=search&id=r00520000619bal01.htm (May 23, 2001).

Don't forget IRC

13. IRC.org. "HomePage". May 23, 2001. URL: http://www.irc.org (May 23, 2001).

Legal Issues:

14. Privacy Foundation. "Privacy Watch". December 28, 2000. URL: http://www.privacyfoundation.org/privacywatch/report.asp?id=51&action=0 (May 23, 2001).

15. Woodward, Victor. "Email,Privacy and the Workplace". 2000? URL: http://www.dominopower.com/issues/issue199809/privacy001.html (May 23, 2001).

16. eff.org. "Active Legal Cases and Efforts". Various. URL: http://www.eff.org/Legal/active_legal.html (May 23, 2001).

17. cdt.org. "Legal Rulings". Various. URL: http://www.cdt.org/ (May 23, 2001).

18. Privacy Foundation. "HomePage". May 23, 2001. URL: http://www.privacyfoundation.org/ (May 23, 2001).

19. Chen, Hans. "Watching the Watchers". September 9, 2000. URL: http://www.vault.com/nr/newsmain.jsp?nr_page=3&ch_id=420&article_id=19332&cat_id=1422 (May 23, 2001).

Monitoring software

20. http://www.download.com and search on keywords: "monitoring" or "filter email web"

21. Chamy, Ben. "A Government Office to Test Web Filters?". August 3, 2000. URL: http://www.zdnet.com/zdnn/stories/news/0,4586,2611649,00.html (May 23, 2001).