Global Information Assurance Certification Paper

GSEC Practical Assignment

V1.4

Patrick Nugent
March 29, 2004

“The Danger Within”

Abstract:

The purpose of this paper is to outline the hidden threats that come from inside a network. These dangers are all too often overlooked because of all the focus on external threats. I will outline what types of threats can come from inside, and explain the difference between non malicious and malicious insider attacks, and offer some tips that can help reduce the risks these users create. I will look at one particular case study showing how susceptible an uninformed user base can be to *Social Engineering* from my personal experience with several administrative users. I will also look at threats that are specific to my environment; an ISP with a large tier two Inbound Call Center.

Introduction: Reading the news

Reading the news, it is apparent that the threat of attack is very prominent. "Hackers" are everywhere. Banks are being attacked[1]. E-Commerce is being attacked[2] [3] Search Engines are being attacked[4]. Even our government is being attacked[5] [6]. It would appear to most that with all of the threats currently circulating on the Internet[7] all of your efforts to secure your network should be placed at the perimeter and faced outwards towards the Internet.

While securing Internet facing systems is CRITICAL to the overall security of your enterprise, it cannot be the only avenue you explore to protect your data. The most common and potentially dangerous threats come from right inside your network, and they can be just as difficult to defend against. Sometimes, these threats are more difficult to defend. The purposes of this paper is to define some of the more commonly overlooked internal threats, as well as help identify some of the more abstract ones.

Internal Threat?

Yes, internal threat. Simply put, anything that an attacker can do from the outside, an attacker can do from inside. Think about what most attackers spend the majority of their time trying to do; access your internal resources. A person who already has access to your internal resources has by default defeated any external measures. They already have access to your internal resources.

[1] Citibank Attack: http://members.aol.com/VCChen/hackedcitibank.html
[2] Amazon DoS Attack: http://www.theregister.co.uk/content/8/17384.html
[3] Coordinated E-Commerce Attack http://www.arstechnica.com/wankerdesk/01q1/greathack-1.html
[4] Yahoo Attack: http://news.bbc.co.uk/1/hi/sci/tech/635048.stm
[5] Government Attack: http://www.newsfactor.com/story.xhtml?story_id=8758
[6] NASA Attack: http://itmanagement.earthweb.com/secu/article.php/1579131
[7] SANS.org Top 20 Threats: http://www.sans.org/top20/

Assessing the risk-Know thy system

The first and most important step to be taken in any plan to defend data has to be the principle of "Know Thy System". You must take the time to understand how your system works in order to correctly identify whether or not someone is using it incorrectly.

Types of Threats

To begin evaluating who may be causing you danger, we should look at what kinds of threats are out there, or should I say "in here".

Malicious Threats

"Wait a minute" you may be saying, "I've read all about '*Black Hat Hackers*'[8] and seriously doubt any master hacker is working here." You may be right. Let's hope you are right, actually. But what does it hurt to look at defending your network as if you knew some "master hacker" was working there?

The malicious threats you will likely face from inside will come in the form of: Disgruntled employees, Nosy people, and the dreaded corporate spy. Let's look at each one:

Disgruntled employees come in many forms, and are basically any person who has a "beef" with the company. It could be pay, it could be feeling unappreciated, it could be working conditions, or it could be having recently been passed over for promotion. If you have employees, there are some that are unhappy. These people will attempt to damage data or seek to obtain information that could embarrass the company or an individual they feel slighted them. The only way you should ignore this threat is to be able to say that your company could not be embarrassed, and no one who works there is unhappy.

The Nosy person is not trying to damage any information, per se. But they will actively seek out information that is not theirs to view.

The corporate spy is a very real threat. A lot of times this threat is dismissed with a simple "I know the people here, no one would do that". The threat of *corporate espionage*[9] is a much larger issue than many people believe[10]. If your company has any information that your competitor would love to have, be it contract info, new products data, sales stats, anything, you face the threat of corporate espionage. The easiest way to access any given piece of information is to place someone on the inside, near it. As mentioned earlier, just by having local access to a network, you have already circumvented a lot of defense measures. This is where the principle of least privilege is vital, as well as auditing success and failure for file access. If you notice that your new mailroom clerk is trying to get into your competitive market analysis folder or your new accountant is trying to look into a file that contains next year's products, they may bear closer scrutiny.

---

[8] Definition by Tech Target.com: http://whatis.techtarget.com/definition/0,289893,sid9_gci550815,00.html
[9] http://security.itworld.com/nl/security_strat/10142003/
[10] Corporate espionage Information and Statistics, http://home.att.net/~dgeusz/corp_espionage.htm

Non-Malicious threats:
"How can a threat not be malicious in intent?" Simply. Complacent and Compliant users can be just as much a danger to the integrity of your data than those who actively seek to destroy it.

The corporate loafer can be identified as a user who, before the Internet, would spend all day at the water cooler. These people commonly do just the bare minimum needed to get by. So how can they be a threat? The biggest way is the fact that they will spend a large portion of the day on the Internet. If given unrestricted and unmonitored access to the internet, their system will be susceptible to all forms of internet spyware[11]. Something as simple as wanting to download new racecar wallpaper could fill their computer with damaging and resource hogging spyware such as Gator[12]. These programs aren't often dangerous in the sense of exposing data, but they do greatly affect individual machine performance and stability, not to mention the affect on network resources with them transmitting their data back to the web site. To combat this, you must first ensure that NO user has administrative control of their local machine in order to ensure that no software can be installed inadvertently. This is not enough however, as some spyware will install itself no matter what access the user has. Using a Proxy Server with web filtering software such as *Surf Control*[13] will allow you to block access to sites in several different ways. You can block sites with access lists, which block specific sites, or with content lists which will block sites with types of content (Adult Content, Games, Casino, etc). Proxy servers will give you a wealth of information about which users have tendencies to use the Internet the most, the sites that your users go to most often and which hours your users are most active online. You must know your system and monitor all traffic that goes to the Internet. There is no more effective way to reduce threats from the Internet, short of not allowing Internet use at all.
The other way the corporate loafer can be a threat is more serious; email vulnerability. This weakness was brought into specific light with the outbreak of the "Melissa"[14] and "I Love You"[15] viruses. The corporate loafer will likely already be conditioned to receive email that is not of a business nature. They will likely be so used to receiving several non-business "joke" emails a day from friends or co-workers. This is the weakness in human nature that email borne Viruses prey upon. They manipulate the virus code to send emails so they appear to come from someone the target would know. If your user base is "used" to receiving cute little animations and running them, the level of threat to an email attachment virus is extremely high. These users will typically not pay any attention to email

[11] Defined by Black Ice as: A general term for a program that surreptitiously monitors your actions. While they are sometimes sinister, like a remote control program used by a hacker, software companies have been known to use spyware to gather data about customers. The practice is generally frowned upon. Source: http://blackice.iss.net/glossary.php.
[12] http://simplythebest.net/info/spyware/gator_spyware.html
[13] http://www.surfcontrol.com
[14] http://www.viruslist.com/eng/viruslist.html?id=3773
[15] http://www.viruslist.com/eng/viruslist.html?id=4010

attachment extensions either; they may not question an executable file (.exe), whereas a diligent employee who usually only gets excel spreadsheets in email may notice if an attachment is a potentially dangerous Visual Basic Script (.vbs). The best way to combat this is to know your system. In most enterprises, the need for users to send or receive executable files is almost non-existent. A quick way to slow this type of spread is to block certain potentially dangerous file extensions, and only allow through attachments with a legitimate business purpose. It is also crucial to explain to department managers why you choose to block certain file types through email. Your programmers may decide that they need to share executable files. In cases like this, you can find creative solutions like creating a share for them to deposit files for review, and restrict access to that folder. Email protection is critical and a large-scale proposition. What your security policy MUST stress is the importance of securing the entire enterprise, and resisting the temptation to risk that security to make it more convenient for a few users. So, now that you have blocked all potentially dangerous email attachments types at your email server, are you finished? No. The corporate loafer will often go to exceptional lengths to receive their "joke" emails. Some will go as far as to configure another mail reader such as Outlook Express with a "home" email account or use web mail services such as Yahoo or Hotmail. Your policy must specifically prohibit this practice, and you must monitor your outbound Proxy Server traffic to help you identify this. If your policy is to block access to certain web sites and block certain email attachments, you must have a clear policy spelling out what specifically will be filtered and you must work closely with your Human Resources department to present a unified front in the event of an incident. HR must agree with and support your decisions to block and filter traffic.

Stressed and Pressed for Time.

A user who falls under this category would be the opposite of the corporate loafer. These are the "go-getters" who are very busy and always trying to do more. You may be thinking, "How can a diligent worker be dangerous? Don't we want to encourage the go-getters?" Yes, you want to encourage them, but consider when most mistakes are made. Most mistakes in any situation are made when the person is not focused. A user who is frequently pressed for time will also likely not show due diligence in protecting proprietary data. A user who is motivated to move ahead will at times take information from your site to their home to "work on later". That data, while not under your control is at risk. Another consideration is how that data is transferred. If the user has a laptop, it will likely be saved locally to that laptop. In the event that laptop is stolen, any data on it is at risk. And this has happened before[16]. It is important to have a system in place where all data is stored on site within your network. Know your users, and what data that may need to be portable. Ensure that only data that is needed on portable machines is transferred. Work with your department heads to ensure that your IT staff provides them with access to that data. A good practice is to map your user's "My Documents" folder to a network location, which is easily

[16] http://www.safeboot.com/safeboot.asp?page=news&area=security

done by right clicking “My Documents” and selecting “Properties”. Under the box marked “Target”, simply enter a network drive path. All items in “My Documents” will automatically be sent to that target location. This protects that data in two ways; 1) it would be backed up in the event of a failure (provided you have a working backup strategy) and 2) the data would only be available on that laptop when it is connected to the network, therefore it could not be compromised if the laptop is stolen. For data that has a legitimate purpose to be portable, you can set up synchronization within that directory, and allow that data to be moved temporarily to the laptop to be used, and then synchronized with the network copy upon the machines return. If this user does not have a portable computer, but still wishes to take information home, they will need some type of media. They would transfer data onto a Floppy, CD, Zip Disk or USB “Thumb Drive”. This is another instance where the principle of knowing thy system is important. You simply MUST know who has CD Burners, Zip Drives or Thumb Drives, and why they need them. It is never a good idea to give someone access to equipment simply because they “want it” (see the following section on “Gadget Junkies”). A good idea is to limit the number of users who are allowed to have CD Writers, such as your help desk, or a departmental contact and have all data copying requests go through that person. If a user wants to transfer data to a CD to take home, they will be more likely to pay attention to it due to the added accountability of having someone else know they have it. This also reduces the risk of someone obtaining data they aren’t supposed to have because they will have another person involved. Then you have to follow it up by ensuring that the media is returned. Making someone sign their name to a “sign out sheet” also goes quite a long way towards making them accountable for protecting it. Sensitive data transferred to removable media is at risk should the media be stolen or lost. A user who is used to taking data home but is also pressed for time will not show due diligence in disposing of that media. It is important to have a policy in place for the disposal of information, and just like it is important to send proprietary paper information through a shredder, floppy disks and CDs full of data should also be properly disposed of. You shred paper to make it unreadable; you should also ensure you destroy any information in other forms. This includes retired backup tapes.

Gadget Junkies are users who like to play with neat stuff. Technology is advancing at quite an impressive rate and there is a lot of really interesting and engaging technology to investigate. Devices and technologies such as Pocket PCs, Camera Phones, USB Thumb Drives, CD/DVD re-writeable drives, Wireless Internet, and many other types of devices are fun to have, but can also be dangerous to allow unchecked into your system. And Gadget junkies will be more aggressive at getting ahold of these devices than a standard user. Any device that allows you to copy data to it to take it with you should be tightly controlled for reasons mentioned in the previous section. Wireless technology, especially in handheld Pocket PCs and PDAs, can be dangerous because they can be connected to a computer on your internal network at the same time being

connected to the Internet, in effect acting as a bridge to your internal Network. It is a good practice to work with department heads to ensure that all technology purchases go through the IT department. Make sure that anyone who wishes to use these technologies makes a strong business case for it, and gets approval from the department head for them. It is important to nurture the relationship with department heads, so in the event that a purchase that could compromise your security is proposed, you can make your case somewhat easier.

The Uncommon Threat:
In your enterprise, there will be a need for some users to have a higher level of access than the majority of the users. Certain people, just by their job function, will need slightly reduced restrictions such as a higher level of access to data, or administrative access to their local machine. It could be a user who administrates a system specific to their department by giving users logins to a system or database, or it could be a user who is responsible for maintaining contact lists of clients for a sales staff. It is imperative to get involved with the department to ensure you understand exactly what these users will be doing so you can employ the principle of least privilege. It may take longer in the beginning to give the user specific access to individual files as opposed to giving them full access to the directory the file is in, but in the long run your system will be more secure.

Another area that you must consider when securing your network from the inside is the user group that typically has the least restrictive access; your Help Desk and IT departments.

Yes, the Help Desk and IT departments. Your most technical users should typically be more astute users and should have a more in depth understanding of how computers and networks work, so logically they would be less likely to make a damaging mistake. But consider what your IT users do on most days. They work with machines that aren't functioning correctly. They work with every piece of data on your network. They work with the physical servers. They work closer to danger than any users, and as such they need to be more careful. Let's look at both.

Help Desk
Your help desk is first in line when a user has a problem. They handle calls on a variety of subjects and at times have to handle a large number of issues quickly. But nowhere in your enterprise is the Principle of least Privilege more critical than right here. You must resist the temptation to give your Help Desk users full administrative control of your network shares. You should instead give them the ability to take ownership of a share to make the needed changes and then to remove themselves from that share. It may seem like a waste of time and resources to make them take a few extra steps to make any changes, but consider this: If a fast breaking virus comes out, the chances of your help Desk falling victim are twice as high. Not only could they potentially get it in their own

inbox, but they could get a user who has it and ask the user to forward the email to them for investigation. And if a Help Desk user has full administrative access to all of your shares and their machine gets infected, guess what? Every one of the shares they are connected to is infected. It can only take a second to go from "bad decision" to "Disaster". This was why the "LoveLetter" Virus was so damaging.

It is also important to make sure you have a clear understanding of what your Help Desk can do and what they should escalate to a Tier 2 team. You may have a Help Desk user who knows a certain registry fix will work, but do you really want to have your Help Desk talking users through the registry over the phone? In a lot of cases, it's best if most users don't even know the registry exists. Some tools like *Remote Desktop*[17], *Microsoft's Systems Management Server*[18], and *Symantec PC Anywhere*[19] allow Help Desk Users to remotely access machines and repair them. But both of these tools allow the user to watch what the Help Desk is doing and the user may make an attempt to do the same thing should another issue arise, thus affecting system stability. You want to be careful what you will allow the Help Desk to do, and what they must escalate.

IT Department/Level 2 support

Your tier two staff, like your Help Desk, is right in "the line of fire". These users typically have more access to servers, network equipment and desktops. And as such, these users are in a position to cause more damage in the event of a mistake. There are some good practices you can employ to minimize the risks. For example, if you have a user who is responsible for backing up data, do not allow them to perform this task with their domain user account. Create a service account and place that in the Backup Operators group, and no others. This way, should that domain user account be compromised, your backups will not be in danger. You must also restrict the number of people who know of that service account and its use. Also, it will be more obvious in your success and failure audits if the service account is being used to log in locally to a machine, thiscan tell you that it has been compromised.

Another good practice is to create a regular account in your domain for your Tier 2 and Help Desk users, and then create another account with administrative rights to the Domain and machines in it. Make it your policy to have your IT staff user their regular account for daily use, and only use their administrative level access account when they are performing an administrative task. Like the Help Desk example previous, if your Tier 2 employees get used to working with a non-privileged account, in the event of a new virus outbreak, the spread to network drives can be minimized.

You should also be sure to have very clear documented steps for your tier two team to take when deploying a new machine anywhere in the network. Whether it

[17] http://www.microsoft.com/windowsserver2003/techinfo/overview/tsremoteadmin.mspx

[18] http://www.microsoft.com/smserver/default.asp

[19] http://enterprisesecurity.symantec.com/products/products.cfm?ProductID=2

is a server or workstation, there should be a minimum standard for a level of protection that must be employed before a machine is attached to the network. For example, you should never allow ANY machine to be plugged into the network without, at minimum full updated virus protection and a certain service pack and patch level. I have seen incidents where a machine has become infected and flooded the network within seconds because the network cable was plugged in without ensuring the most recent Operating System patches were applied. The vulnerabilities that those patches would have fixed were left exposed, causing network issues, exposing data and adding work to fix the machine, all of which could have been easily avoided with a few extra minutes of diligence. In the case of a server being built and added to the network, you should have a clearly written document stating which steps need to be taken to secure the server such as which patches to apply, how to configure the Virus protection, which services to exclude, and which system policies to apply. Once the server is built following these guidelines, you should have another person review the configuration, prior to deployment.

A brief detour into social engineering:
All of the subjects covered to this point have been somewhat general. Now I'd like to go into an experience I had with obtaining the passwords of six directors and VPs by using simple Social Engineering.

First off, what is "*Social Engineering*"[20] ? In short, it is the ability to coax information out of people that may help you in attacking and compromising data. This tactic is as old as "Hacking" itself, from *John Draper*[21] (Aka: Cap'n Crunch) who used Social Engineering to learn the phone switching system in use, thus allowing him to make free phone calls by manipulating the tones the Public Phone system used to Kevin Mitnick who used Social Engineering to obtain information which allowed him to target the specific data he was seeking, and generate his attacks; As Mitnick wrote in his book, The Art Of Deception: Controlling the Human Element of Security[22]; "*Rather than using a crowbar to break in, the social engineer uses the art of deception to influence the person on the other side of the door to open up for him. "*. Social Engineering is generated from outside, so some may consider it an external threat. But the people who make Social Engineering an effective way to gather information are usually inside. In both cases, the information Mitnick and Draper needed was obtained from insiders.

This case started simply enough with me having to visit a user who was having a specific problem. The user was the admin assistant of the Divisional VP. While working at her desk, I noticed a note pad. Thinking back to the previous time I worked on this user's desk, this same notepad was in the same place. I looked

[20] http://www.securityfocus.com/infocus/1527

[21] http://www.webcrunchers.com/crunch/Play/history/home.html

[22] **Publisher:** John Wiley & Sons; 1 edition (October 4, 2002)

closely at the notepad and noticed that the VPs network password was written on it, as well as his last three which had been simply crossed out. This was an obvious danger, but it raised a more important question in my mind. “How many of these other Admins know their boss’ passwords?” So I decided to answer the question for myself. This particular office had five Administrative assistants who supported six Directors and VPs. What I found surprised me, and led to some strong changes in our policies.

The set up was this; I had someone call each of these administrative assistants to attempt to get these passwords. I armed this person with only the name of the Director or VP (readily available from the corporate website) the phone number of the Director or VP (Readily available by calling the main number posing as a salesman or client) and the “hook”, which in this case was “I am calling from the Help Desk and we’re setting up _____’s new laptop, I need his password to configure his/her mail.”

In each case, for each of the six directors/VPs, not only did the Admins know the passwords, but they readily surrendered them without obtaining permission from the Director or VP in question. Not once did any of the admins question the “new laptop” nor did they even ask the name of the person “calling from the help desk”. They did not question (or understand) why the “Help Desk” would be installing any software on the machines when the policy at our company is for all new hardware setups to be completed by Tier 2.

So what did I learn?

- First and foremost I learned that being aware of your surroundings could lead to huge discoveries of threat (just being aware of the notepad).
- I learned that our current system of ordering equipment had little to no control built into it. We had gotten caught in a trap of people being able to arbitrarily order equipment, thus making it nearly impossible to identify when anything out of the ordinary occurred. No Administrative assistant should be “surprised” to find out his or her boss is getting a new laptop from anywhere. And subsequently, no Help Desk should be surprised to hear that someone is having trouble with a “new” computer that the Help Desk was not previously aware of.
- I learned that we had no specific policy forbidding the Admins to have the passwords
- I learned that we had not effectively communicated to the user base the dangers of this practice, including the VPs. This made the users complacent. We had never taken steps to help them realize what danger was in being complacent.
- I learned that the reason the VPs gave their passwords was because the Admins liked to have the VPs and Directors’ PCs logged in when they arrived at work. This threat to security came about because they wanted to save the VPs a few seconds in the morning.

- I learned that none of the Admins thought it was enough out of the ordinary to follow up with IT about the “new” laptops.

How did we correct it? Well, the first reaction could have been to reprimand the Admins, but without a specific policy forbidding it enforcement was not an option. So first we looked within the department at the specific policies and processes we had that made this possible. I met with the entire department and as a team:

- We initiated a re-write of security policy that specifically forbids the sharing of passwords under any circumstances.
- We looked at the equipment ordering processes and created a web form from the Intranet site that users can fill in data relating to the software needs for each new computer that IT is setting up. In the event a new computer is purchased, the user who will be getting the computer will be emailed a link to that site and asked to complete the form. This eliminated the “surprise” of any new PC setup. No user should ever be unaware that a PC is coming. In the case of VPs and Directors, the Admins would be authorized to fill out the form on behalf of their boss.
- We created a procedure document within the IT department stating that when any machine is set up, the final configuration of profile specific configurations such as email where the user’s password is needed will be done by Tier 2 with the user present or with the user over the phone via SMS or Remote Desktop.

Now that we had narrowed down our internal procedures and policies to minimize this specific risk, we met with the Directors and Admins and explained the danger. We went over the Security Policy changes and explained which steps we were taking to reduce the risk on the back end. In these meetings we asked for specific buy in from the Admins and the Directors/VPs. It was in these meetings that we discussed the critical nature of protecting the data, and explained the potential for critical information to be compromised.

- We asked them to communicate to all people within their departments what the new technology ordering process was, and why it was important.
- We asked for their support to initiate user education initiatives in the form of Intranet Site information and department head meetings in an attempt to raise awareness enterprise-wide of security policies. With this directive coming from the top, we agreed it would carry more weight.
- We asked for specific support in regards to the Admins notifying the IT department whenever unusual events occur. We asked them to not think of it as “bothering us”, but rather “informing us” of anything out of the ordinary. As in any crisis, early detection helps stem problems.
- We explained to the VPs the reality of Corporate Espionage and showed the VPs how easily we could have accessed things like Salary Reports, Future Product Plans, and Sales and Tax figures. Making the VPs aware that anything they had access to, their password had access to was quite eye opening to them.

The meeting, while daunting, was quite productive. We had to be very careful not to be accusatory, but rather show how dropping our collective guard for even a second could be disastrous and embarrassing to the company. There were a lot of positives that came out of that meeting as far as policy changes and commitments to user education. But perhaps the greatest thing to come from the meeting was getting the Executives to put the security of our data on their list of priorities.

And while the overall outcome was positive, looking back there is something else I should have done. I had never obtained written permission to attempt the project. I should have been in contact with both my Human Resources and Information Protection departments to get permission to carry out the experiment.

Putting it all together; tips to help reduce the risk

So now that you have learned of some of the threats, here are some of the more common things to look at to help you reduce the risk from inside:

Audit your files.

- You must audit the files that hold sensitive information. Auditing file access has the potential to overwhelm you with data. Following the principle of Knowing Your System, you should be sure to understand what data is the most critical for you to protect. In some cases it will be obvious (Payroll Files, Customer Contact) and in others not so obvious (New product data, Documents relating to upcoming projects/budgets). A good rule of thumb is to think "What data would my biggest competitor love to have?" This will lay good groundwork to help you determine your "highest priority" data to audit.
- The first audit you need to set up is a failure audit, which audits and logs every attempt to access a particular file or share. This will help you determine if there is a particular user account that is trying to get into files they are not supposed to. This can tell you if a particular user is trying to do it, or it can tell you if a particular user account is compromised and being used.
- On the other hand, you need to be sure to also do a "success" audit. This type of audit will tell you who successfully gained access. It is important to know if an unauthorized user failed to get into sensitive files, but it is even more important to know if they finally succeeded.

Keep track of your user accounts.

- Make sure you have a solid policy regarding a naming convention for what your user accounts are. This is important because without a standard for user accounts (for example *first initial/last name*), you will have a very difficult time identifying unauthorized accounts being created.
- A good practice is to have an IT user go through at least once a week and verify that all active user accounts are valid, making sure to deactivate any unidentified accounts and accounts of users who have left the company or are on leave. It is not recommended to delete accounts, just in case the accounts have a legitimate reason for being.

- Be diligent with group affiliations and control access to ALL resources by group policy. The reason for this is two fold; 1) it makes it all the more obvious when a single user gains rights to sensitive data, and 2) it streamlines your ability to control access to information based on job function. In a Windows environment, there are no limitations on how many groups a given account can be in, so you can get very granular in your approach to granting access. For example; if you have three accountants who need access to view certain payroll files, you can create a specific group for the accountants and grant that group the ability to read only the files they need to read instead of an entire directory.
- Another good practice is to make sure that no accounts that have administrator access look any different than standard domain user accounts. If a user in your domain named Kevin Jones has an account of *kjones*, an administrator named Kevin Jones should not have an account of, say, *admin-kjones*. You should also avoid identifying user accounts by department, such as *HR*-kjones. The reason for this is that if an attacker gained access to your system, they would seek out accounts easily identified with administrative access, or that would logically have access to the information they'd most likely want to access.

Understand the user's job functions.

- Know what the user base needs in order to do their job. If you have a large group of users who work in a call center capacity, you should evaluate their communications needs. If the users do not need email, no email client should be installed. If the users have no need to print any information, place their accounts in a group that denies print functionality. Another good question to ask yourself is; "Do the users need floppy drives?" Floppy drive access can easily be denied within group policy, and can offer you two levels of protection; 1) it can protect you from users bringing in viruses from their home PCs and 2) it can protect you from having sensitive data copied and taken off site.
- By the same token, ask yourself if the user needs access to certain areas of their PCs, such as the run command, the Windows Control panel, CDRom drives, or even direct access to the hard drive. Disabling any or all of these items can protect you from varying levels of malicious and inadvertent danger. For example, if a user has a malicious intent to damage their local computer, not having access to tools like the Windows Registry Editor (regedit) or a DOS command line make damage more difficult.
- Email is another area where there are a lot of opportunities for protection, and you should spend some time understanding what users need to do their job. The most damaging viruses in history such as the previously mentioned Melissa and LoveLetter, as well as internet worms *So Big*[23] and *Blaster*[24] spread through email attachments. Understanding the types of

[23] http://www.viruslist.com/eng/viruslist.html?id=58906

[24] http://www.viruslist.com/eng/viruslist.html?id=3720

attachments that users need to receive will help you determine which types to allow through your email server.

These are just a few of the ways that you can look within your system to begin to identify the dangers that are out there. It is by no means meant to be a comprehensive list.

It is also imperative to know your environment, and the dangers you may face that would be specific to it. For example, my environment is a large ISP that includes an inbound call center filled with Tier 1 customer support associates. In such an environment, I must be aware of certain dangers that many organizations may not ever have to face. In an environment with so many technical employees each with their own level of expertise, we are more at risk from things such as:

Disgruntled employees; If the inbound call center employs over 200 and the internal IT department employs 10, you can bet that somewhere in the call center are employees who feel slighted by not being moved up to Internal IT. When a position becomes available, there is frequently a move of over half of the call center applying for the position. Just by the law of averages, someone is going to get a job that someone else will think they are more qualified for. This leads to situations where upset users are either angry and want to maliciously attack data or want to damage the machine in an attempt to show that the person who got the job "can't fix it".

Users who spend all day fixing computer problems for customers often spend a lot of time trying to figure out ways around things like proxy restrictions or administrator passwords. "Techies" usually come across things at home that they want to share with people at work, but are restricted by the web filtering software. Rather than forget it, often they will feel compelled to try and work around it.

Technical users, much like IT Department Staffers mentioned above, are at times in a position to make more visible mistakes. They often believe they know a bit more (and usually they do), and as such will go further trying to fix things before asking for help, potentially leaving systems in a vulnerable state.

Techies will also often be the "Gadget Junkies" and have all the neatest toys.

Another uncommon issue is web logs. Microsoft Corporation recently terminated an employee for posting pictures from inside the Microsoft Campus[25] in their online journal. This issue is very complex, and could be debated for hours, and as such the specifics of it are outside the scope of this paper. But it does raise a very serious question; could potentially sensitive information be leaked out by someone writing an online journal? Yes. Just as easily as someone talking at a party could expose information about your organization. It is a good idea to review your security policy, and if you specifically prohibit the dissemination of information through channels like verbal communication or email, it would be a

[25] http://www.michaelhanscom.com/eclecticism/2003/10/of_blogging_and.html
http://yro.slashdot.org/article.pl?sid=03/10/29/1421223&mode=thread&tid=109&tid=187

good idea to specifically mention web logs and personal web pages as other avenues where information sharing is forbidden.
Being an ISP that provides wireless product to its customers, we often run into issues where marketing and sales people want to use a wireless router in their offices. The issue this creates is this creates a wireless access point, and with more and more laptops coming with integrated wireless cards it can create a bridge between internal networks and the Internet. A computer can be plugged into the internal network via the Network Interface card while the wireless card is picking up a live Internet address from the wireless router. Should that computer become compromised, your entire network is at risk. But it is not feasible to deny users access to the very products they are selling. The way we worked around this is to set up wireless products in lab environments for users to test and learn with, but that still fall under IT department control.

Summary: Standing on the front porch looking in.
Securing a network from threats that come from outside is an intensive job with lots of details that need attention. But as you have seen there are just as many, if not more, threats coming from inside your network. As with external network security, an expectation of "complete" security is unrealistic, but you can significantly reduce the level of risk by taking a step back and seriously evaluating your network. I hope this paper has given you a roadmap of things to look at as you start the process. But it cannot stop there; too often we get into the trap of "going down the checklist" and moving on to the next issue. I had completed an audit of all of servers a few days before discovering the VP Password on his Admins desk. And up until the moment I found that password, I had been feeling pretty good about our security. The lesson learned is that you can never let your guard down; you can never allow yourself to be complacent. Now, I spend a great deal of time reading news stories about large scale issues in other organizations, and looking very carefully at my own system to see if I am at risk. It is very rare when an incident occurs to hear an Administrator say, "Yes, I had thought about that." We get blindsided by things in this business. But by following some simple guidelines we can minimize the impact of those incidents. In regards to internal threat, the SANS cornerstones of Principle of Least Privilege and Know Thy System are critical.

The good news is; you can increase the overall security of your system. By employing a lot of the techniques discussed here our organization was able to keep the system available during the spring 2003 outbreak of the *SoBig* worm. We were the only location corporate wide that was able to stay available. We were adversely affected, but the impact this particular outbreak had on our overall system was considerably lighter than our counterparts faced. We considered that a major victory in the battle to protect our data.

Reference Links

1: Victor Chen; “The man who hacked Citibank”, May 1998
http://members.aol.com/VCChen/hackedcitibank.html

2: Thomas Greene, Register UK, June 2001
http://www.theregister.co.uk/content/8/17384.html

3: Arian Evans; “The Great Hack Attack”, ARS Technica
http://www.arstechnica.com/wankerdesk/01q1/greathack-1.html

4: “Yahoo Brought To Standstill” BBC News, February 2000
http://news.bbc.co.uk/1/hi/sci/tech/635048.stm

5: Dan Gebler “US Governement Computers Widely Hacked in 2000” Newsfactor.com, April 2001
http://www.newsfactor.com/story.xhtml?story_id=8758

6: Sharon Gaudin “NASA Reportedly Hacked Hours After Columbia Was Lost” Earthweb.com, February 2003
http://itmanagement.earthweb.com/secu/article.php/1579131

7: SANS.org Top Twenty Vulnerabilities, October 2003
http://www.sans.org/top20/

8: Techtarget.com definition “Black Hat Hacker” 2000-2004
http://whatis.techtarget.com/definition/0,289893,sid9_gci550815,00.html

9: Secutiry.itword.com “Corporate Espionage; When Competition Goes Too Far”, October 2003
http://security.itworld.com/nl/security_strat/10142003/

10: Bob Sullivan; “’Netspionage’ costs firms millions”
http://home.att.net/~dgeusz/corp_espionage.htm

11: BlackIce.iss.net Glossary of Terms “Spyware”.
http://blackice.iss.net/glossary.php

12: Simplythebest.net Glossary “Gator Spyware”
http://simplythebest.net/info/spyware/gator_spyware.html

13: Surf Control Web and Email Filtering Software, 2003
http://www.surfcontrol.com

14: Viruslist.com, Virus encyclopedia “Melissa”, March 2004
http://www.viruslist.com/eng/viruslist.html?id=3773

15: Virsulist.com, Virus encyclopedia “Love Letter, aka ‘I love you’”, March 2004
http://www.viruslist.com/eng/viruslist.html?id=4010

16: Safeboot.com, Mobile Data Security News
http://www.safeboot.com/safeboot.asp?page=news&area=security

17: Microsoft.com “Remote Administration of Windows Servers using remote desktop for administration” March 2003
http://www.microsoft.com/windowsserver2003/techinfo/overview/tsremoteadmin.mspx

18: Microsoft.com “Systems Management Server”, March 2004
http://www.microsoft.com/smserver/default.asp

19: Symantec.com “Enterprise Solutions, PCAnywhere”, 1995-2004
http://enterprisesecurity.symantec.com/products/products.cfm?ProductID=2

20: Techtarget.com Glossary of Terms “Social Engineering”, March 2004
http://searchsecurity.techtarget.com/gDefinition/0,294236,sid14_gci531120,00.html

21: Captain Crunch (John Draper), Webcrunchers, Intl. 2003
http://www.webcrunchers.com/crunch/Play/history/home.html

22: Kevin Mitnick: “The Art Of Deception”, Page 180. Published October 2002, Wiley and Sons. ISBN: 0471237124

23: Viruslist.com, Virus encyclopedia “SoBig”, March 2004
http://www.viruslist.com/eng/viruslist.html?id=58906

24: Viruslist.com, Virus encyclopedia “Blaster”, March 2004
http://www.viruslist.com/eng/viruslist.html?id=3720

25: Slashdot.org “Microsoft Fires Mac Fan for Blog Photo”, October 2003
http://yro.slashdot.org/article.pl?sid=03/10/29/1421223&mode=thread&tid=109&tid=187

Last Updated: July 21st, 2017

Upcoming Training

SANSFIRE 2017	Washington, DC	Jul 22, 2017 - Jul 29, 2017	Live Event
SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
Community SANS Omaha SEC401*	Omaha, NE	Aug 14, 2017 - Aug 19, 2017	Community SANS
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
Community SANS Trenton SEC401	Trenton, NJ	Aug 21, 2017 - Aug 26, 2017	Community SANS
Virginia Beach 2017 - SEC401: Security Essentials Bootcamp Style	Virginia Beach, VA	Aug 21, 2017 - Aug 26, 2017	vLive
Community SANS Pasadena SEC401 @ NASA	Pasadena, CA	Aug 23, 2017 - Aug 30, 2017	Community SANS
Mentor Session - SEC401	Minneapolis, MN	Aug 29, 2017 - Oct 10, 2017	Mentor
SANS San Francisco Fall 2017	San Francisco, CA	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS Tampa - Clearwater 2017	Clearwater, FL	Sep 05, 2017 - Sep 10, 2017	Live Event
Mentor Session - SEC401	Edmonton, AB	Sep 06, 2017 - Oct 18, 2017	Mentor
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
Community SANS Albany SEC401	Albany, NY	Sep 11, 2017 - Sep 16, 2017	Community SANS
Mentor Session - SEC401	Ventura, CA	Sep 11, 2017 - Oct 12, 2017	Mentor
Community SANS Columbia SEC401	Columbia, MD	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Dallas SEC401	Dallas, TX	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Boise SEC401	Boise, ID	Sep 25, 2017 - Sep 30, 2017	Community SANS
Baltimore Fall 2017 - SEC401: Security Essentials Bootcamp Style	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
Community SANS New York SEC401	New York, NY	Sep 25, 2017 - Sep 30, 2017	Community SANS
Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
SANS DFIR Prague 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
Community SANS Charleston SEC401	Charleston, SC	Oct 02, 2017 - Oct 07, 2017	Community SANS