Global Information Assurance Certification Paper

Dude, Where's My IT Policy

GIAC Security Essentials Practical Assignment
Version 1.4b

By

Steve Friedman

March 2, 2004

Abstract

This Practical Assignment will focus on the development of the IT policy and how it applies to the general staff in an organization, the responsibility of the staffs knowledge and understanding of the policy, and protection of the company's recourses by having a complete understanding of the policy and knowing when and how to it applies to them. An effective IT policy is only successful when those that it applies to comprehend the full meaning of the policy. This paper will provide best practices for developing an effective IT Policy, getting senior management to "buy into" the importance of the policy, and educating the staff so that they have a full understanding of the policy and its importance.

While having a solid IT Policy in place is a big step in the right direction towards securing your network, and creating an abuse free environment, it is only just that; a step. Without every member of an organization understanding the policy and understanding what role they themselves play in its effectiveness, your policy will not serve the purpose you envisioned when creating it.

Note: This paper assumes that from a technology perspective, all security, monitoring, analysis and backup & recovery systems are in place. The IT Policy that is discussed in this practical refers to the policy for day-to-day functions and responsibilities of the non-IT staff.

Introduction

In today's world of business, so much responsibility falls on the shoulders of the IT professional to create and maintain an environment that is both secure from internal/external threats, and free from abuse of its resources by employees. It is a large and unfortunate misconception, that a company with a competent IT staff, and a plethora of hardware/software IT security and monitoring products can create an environment that is free from today's all too common threats and abuses.

So what does this all mean? That no matter how skilled an IT dept. an organization employs, and no matter how much money they throw at technological solutions to fight these threats, that they have no choice but to be left vulnerable? Wrong! A critical building block in an IT infrastructure is the IT policy. This leads us to two types of organizations; those who have no policy in place, and those who spend time creating an IT policy, and then leave it up to the IT staff to enforce. It is critical, that every member of an organization, from managing partner, to mail room clerk, have not only a full understanding of the policy in place, but also a full understanding of the purpose of the policy, and their responsibility to follow it.

In the day and age that we currently live in; viruses, worms, DOS attacks, and unauthorized access due to results of social engineering are events that are becoming all to common. From a technology standpoint, there is only so much that can be done to protect a firm and its resources.

What is an IT Policy?

An IT policy is a set of rules and guidelines to protect resources and information. It sets the rules that all staff (including IT personnel) are expected to follow. It establishes authorization for the IT staff to monitor, probe and investigate activities within the organization, and defines the consequences of those activities.

A good IT policy will also include a section to protect its people. How can an IT security policy protect a person you ask? Anyone in an organization who is responsible for information needs to know what actions to take when a situation arises that could possibly subject company resources or information to compromise. An effective IT policy should provide enough information so that an employee can act accordingly in a situation to help protect an organizations resources and information. The IT policy sets the guidelines for protecting an organizations resources, information, and people, and states what is allowed, and more importantly what is not allowed.

Who needs an IT security policy?

The answer is, who doesn't need an IT policy? Whether you are a global organization, with 2000 servers and a WAN that spans four continents, or you are a one site fifty user LAN, you need an IT policy. Technological safe guards will only do so much. Sure, you may have anti-virus software, a firewall, and a ton of other security applications/devices in place, but the weakest link in any security infrastructure is always going to be the "human factor".

Sure your firewall is blocking you from external SYN flood attacks, and your anti-virus software (that is updated with current definitions), is guarding you against the latest virus/worm that is floating around the net, but do your users know that they shouldn't load 3rd party software on their machines, or that giving out their username and password to ANYONE is a big no no (see the section that discusses social engineering later in this paper)?

So how can you convince your senior management/owners that your organization requires an IT policy, take a look at some of the results from the CSI/FBI 2003 Computer Crime & Security Survey:

- 92% of respondents to the survey sited some sort of attack or misuse (DOS attack, unauthorized access by insiders, abuse of Internet access, sabotage, etc…) in the last year
- 75% of respondents cited financial loss as a result of attack or misuse
- Theft of proprietary information resulted in a loss of $70,195,900.00
- 99% of respondents surveyed used anti-virus
- 98% of respondents surveyed used firewalls

Look at those last two items; basically all the respondents to the survey used some form of hardware/software solution to protect their organization from harm and still reported financial loss. Technological solutions to these problems are just not good enough

Developing the Policy

It is a must that you keep a few things in mind when developing your IT policy:

Risk Assessment

Before you write your policy, you have to figure out exactly what threats and in the impact of each threat that you are trying to protect your organization from. This is done by means of risk assessment.

There are two categories of risk assessment that one can choose from:

- Qualitative – assign risk categories (e.g. high, medium, low)
- Quantitative – assign values based on two things, **1**. The likelihood and probability of the threat occulting in your environment, and **2**. The magnitude of the impact of the threat.

Seeing as we are trying to create a policy that encompasses all threats that could compromises the integrity of the corporate IT infrastructure, the Quantitative approach will work best, as any risk that results in a significant impact should be analyzed, protected against and included in your policy.

The following are two examples of threats, and the impact of those threats:

Threat – Viruses spread by email

Most of today's viruses and worms that are wreaking havoc throughout the Internet these days are spread via email. Even with a good enterprise level anti virus software solution, there is still a threat of infection. Users may receive a seemingly harmless email from someone they do not know, open it up, and within minutes the latest virus or worm has made its way through your organizations network.

Impact – Viruses spread by email

Last year alone, according to the 2003CSI/FBI Computer Crime and Security Survey, companies reported losses of over 27 million dollars due to the effects of computer virus infection.

Threat – Social Engineering

Most people today rarely verify whom they give information out to over the phone. An effective social engineer can punch a whole right through your IT security infrastructure, before they even actually sit down at a computer.

Impact – Social Engineering

An attacker with a valid set of user credentials to your organizations computer system can not only steal, manipulate, and delete data, but can also do it undetected because he/she is using valid credentials.

These are just two examples or threats to look at when performing risk assessment, but you'll want to make sure that that you are very thorough in this process, as this is the basis for the overall contend of your IT policy.

You cannot create an IT policy on your own!

But what do you mean? I am the Director of IT for a fortune 500 company, if I'm not the person for the job, then who is? The answer to this question is simple, AS MANY PEOPLE AS POSSIBLE! Now it's not expected that you go and sit with every single employee in your organization and ask them what they think should be included in the policy, but you should meet with a representative from each decision making group of the organization, and of course "day to day" end users who will have a say in how usable (or unusable) your policy is. For the following reasons, you should meet with:

- **President/CEO** – Never try to create or change an organizations policy without first talking to the person who is ultimately in charge. The main reason for this is that everything flows downwards in a company; you need to get the top person to "buy in" to your policy.
- **Legal dept**. – Make sure that you clear everything you put in your policy with your companies legal dept. The absolute last thing you want your policy to do is break the law. You can't protect your company if you put a policy in place that is violating the rights of the staff, or contains guidelines that in and of them selves are unlawful.
- **A manager from each dept**. – You want to make sure that your policy is equally effective in all areas of your organization. You want to put measures into place that apply to the entire organization, but do not restrict anyone from being productive. For example, Human Resources may not have any reason to download via FTP, however, your bookkeeping dept. may need to download program updates monthly via FTP.
- **End users** – Meet with a group of end users, and ask them to review your policy. Now while they may turn red with anger when you tell them that all access to AOL is being blocked at the firewall, they will be able to tell you whether or not the policy you are trying to put in place prevents them from performing the day to day functions of their role in the organization.

What should an IT policy contain?

There is no such thing as a "One size fits all" IT policy. What works for one organization, may not work for another. There is really no limit to what an IT policy can contain, but remember this; you are trying to provide the highest level of security while still maintaining a productive work environment. Never make your policy so restrictive that you are preventing someone from accomplishing the job they were hired to do.

The policy while being tailored to your organizations specific security should contain the following basic elements:

Mission Statement

It is important that when people read the policy, they understand what you are trying to achieve. Simply writing a numbered set of rules as to what staff should and should not do won't gain you much support. Take the time to explain the goals you are trying to reach with the policy, why it's important that it is followed, how following the IT policy affects them and ultimately creates a better work environment. Make it clear that if for any reason someone is not sure about something in your policy that they should not hesitate to contact someone in an authoritative position who can clarify it for them. Your mission statement shouldn't be more then a paragraph or two.

Accountability

This is a nicer way of saying "consequences". While you don't want to come across as an evil dictator, you also need to show the seriousness of your policy and the accountability that one will be held to if he/she does not comply with it. Careful how you word this, you don't want people to be afraid of coming forward if they see or suspect something, or if they themselves made an error and mistakenly violated the policy.

Computers

Most, if not all users in your organizations are going to have a computer, or at the very least, access to a computer. Whether it is a desktop that remains in the office, or a notebook that they take in the field/home with them, users should know that along with the resources they are given, there are some basic responsibilities that come along with it:

- **Always make sure that the computer is locked when away from it**

  Leaving a computer logged on and unattended can let anyone gain access to company resources using your account. While this is a rare problem, it is still a good idea to lock your workstation when leaving it unattended, after all, you wouldn't leave you're car running with the doors wide open in a parking lot, would you?

- **If you are a notebook user, the notebook must remain in your possession at all times, lending a notebook to another staff member, or a friend or family member is something that should NEVER be done**

  If the notebook is out of the possession of whom it was issued to, then there is no way that its use can be accounted for. The equipment that you issue to the staff is issued for the specific purposes of business use. Who knows what a family member or friend is going to use this computer for, what changes to the configuration will be made, and what kind of damage it will incur.

- **Under no circumstances should any software that is not explicitly approved by the IT dept. ever be loaded on an issued computer**

  Most users go under the assumption that their computer is just that; their computer. Unless you tell them not to, it is safe to assume that they will load whatever programs they wish to on it. This can result in software conflicts, time wasted via instant messaging programs, and even lawsuits. Yes you read that last part correctly. One of the most common applications in use today are file sharing programs, and if a user in your organization gets caught downloading pirated copies of Microsoft Office, guess who is held responsible?

User Accounts/Passwords

As an IT professional, you can take many measures to ensure the integrity of your user accounts. You most likely have a 90-day (or less) password expiration date, a minimum set of mixed alpha-numeric characters that users must choose from, and a password history. All these measures that you are taking will accomplish absolutely nothing if users in your organization write their password down on a post-it and stick it on their monitor, or give their account information to anyone who asks for it.

Explain in your policy that there is never a need for anyone else to have his of her password. This goes for the IT dept. as well. If IT really needs to get into someone's account, they can reset the password. The integrity of the account is preserved only with the user being the only person with knowledge of their password.

Email

It is important that you include best practices on proper use of the email system. You should provide a list of best practices for use of the corporate email system; these practices should include, but are certainly not limited to:

- **Do not sign up for any email lists or online subscription services that are not related to business purposes**

  Signing up to receive emails on weekly movie show times may seem harmless. But most marketing companies buy email distribution lists and resell them. This could cause your organization to receive huge amounts of unwanted emails (spam).

- **Do not give out your email address or the email address of anyone else in the organization, unless you can verify who you are giving it to**

  As with the previous point, giving out your email address to anyone who asks for it, is a sure fire way to end up on junk email distribution lists.

- **Do not forward jokes, chain letters, or any other type of correspondence that is not related to business purposes**

  Not only is this a huge waste of time, and space on your email server, but as you will read below, there are legal ramifications if the emails being sent contain questionable content.

- **If you receive an email that you are unsure about it's contents, contact a member of the IT dept. immediately**

  Even though you are running anti virus software, there is still a risk of infection. It's a good practice to let users know that if they are unsure of an email they receive, they should contact a member of the IT dept. Immediately.

I know what you're saying, sure are a lot of "Don'ts" on that list, but following these recommendations will lead to more productive use of the corporate email system. It should be stated in your policy that the email system is for "business purposes only".

Aside from the lost productivity that your company will experience due to employees using the email systems for personal use, there are also some legal issues to keep in mind. According to a report released last year on corporate email systems by IDC:

- 10 Percent of US employers have been subpoenaed in lawsuits to provide employee emails
- 8 Percent of companies have been hit with discrimination and/or sexual harassment charges stemming from email misuse

Employees forwarding jokes or other such inappropriate material around the office can end up costing you more then just time and lost productivity.

State it very clearly in you policy that all messages sent through the corporate email system are subject to monitoring. *

Internet

The development of the Internet has given organizations a most valuable research tool. Unfortunately, it is not often used that way. Out of all the resources available in modern business today, the Internet is by far the most abused. These abuses include users viewing illicit material, checking their personal email, playing games online, gambling, visiting online dating sites and just simply wasting time by browsing material that is unrelated to business purposes.

You need to make it very clear in your policy that this is something that is not acceptable.

State it very clearly in your policy that you monitor all Internet traffic and make sure that you review your logs on a weekly basis. *

Data Storage

At the heart of your IT policy, you are trying to protect your organizations data. So you should make it clear where and how all data should be stored. Some people may not see anything wrong with storing all data on the local hard drive of their computer. But what happens if this person's notebook gets stolen, or their hard drive crashes, or any other situation in which data recovery would become at best difficult and at worst impossible.

State it clearly in your policy where data is to be stored on the network.

Giving out Information

It may seem silly or even inappropriate to contain a section in your IT policy about giving out information. But even the most seemingly harmless detail can cause severe problems for an organization.

State in your IT policy that under no circumstances should a user ever give out any information to an outside or unknown source, that relates to the organization.

Why is this important? I mean what harm could it do if a user were to accidentally send someone an organizational chart or an internal directory listing? Consider the following true story of how a social engineer wreaked havoc in the mid-sized accounting firm that my friend works at.

Note: all company info and names have been changed

Their receptionist got a phone call from a female caller in the AM that seemed innocent enough.

Receptionist "Thank you for calling Armstrong and Associates, Mary speaking how can I direct your call?"
Female Caller "Hi Mary, I was in your office last week meeting with Mr. Armstrong, and I gave something to your mail room clerk to mail for me, turns out that the recipient never got the letter, can you transfer me to the mail room so that I can just follow up with him."
Receptionist "Sure I'll transfer you right over, his name is Mark."
Female Caller "Great thanks Mary, I really appreciate it".
Mark "Mark speaking."
Female Caller "Hi Mark, this is Kristen Armstrong, Bob's sister, I just got off the phone with my brother, he's on his way over here, and he wanted me to call to ask if you could fax over the company directory listing, you know the ones with all the direct phone extensions and email addresses."
Mark "sure, no problem, Bob's always working, he's got to be able to get in touch with his staff."
They both laugh
Female caller "Thanks again sweetie, I'll make sure that Bob knows how helpful you were."
Mark sings to himself "moving in on up" as he faxes over the complete company directory information of Armstrong and Associates to Bob's sister

The very next day every employee in the company started getting phone calls and emails from a direct competitor. By the time management had realized what had happened, it was too late, and within the next month 3 staff members ended up leaving to go and work for the competitor.

Aside from the part about Mark singing to himself, this is exactly what happened. This is not from a movie and it is not excerpt from Kevin Mitnicks "The Art of Deception". This really happened to someone I know.

Make sure that you state in your policy that any type of information in regards to the organizations staff and/or clients should ever be given out without verifying where it is going. In my friends story, all Mark had to do was call up Bob and clear it with him first, this would have saved the company 3 good employees that were lost to a competitor, and would have saved Mark his job (he was terminated a week after the incident).

** As I stated in a previous section of the paper, you should clear any verbiage that goes into your policy with your legal dept. especially when it comes to monitoring emails/network activity, and Internet access. Last thing you want to do is violate anyone's rights*

Now what?

Sell it!!!

Once your policy is written, you will want to have the senior management/owners look at the policy. This is important so that they can make their comments and suggestions, and it also provides you with the opportunity to get them to "buy into" the Policy. You need to take this opportunity to sell the IT policy to them. Stress its importance. Make them understand. Create fictitious scenarios in which users do not follow the policy, and as a result caused downtime, lost productivity, and ultimately financial loss. Scare the heck out of them. The IT policy should have the full support of the top brass in any organization. Remember, it all flows downwards

Test the policy

As with any new technology, process, or procedure, you will need to test your policy. A new policy in essence is a stimulus for an organizational change, and the initial reaction of the change will need to be analyzed. The effects of the policy must be looked at in order to know if the goals of the policy you set out to achieve were in fact met. You may find out that your policy was in fact too restrictive, and you may need to make several revisions before you can release your policy to the masses.

Any policy that people don't understand, they are not going to buy into, and if they don't buy into it, they aren't going to follow it. If you want your IT policy to be a success, then it is critical that you take the time to help everyone in the organization understand not only the content of the policy itself, but also the reasoning behind it.

Unveil your Policy

Unveil your Policy by way of any medium you wish, email it, put it on your organizations intranet, or even print out copies for people to read.

But in no way should this be the final step. People will most likely have questions, and chances are they aren't going to come to you until after there has been a violation of the policy. So it's up to you to take the initiative and go to them, as with the actual technical aspect of IT, you want to be proactive, not reactive.

If you can, meet with the staff in small groups. People are more likely to come forward with questions or concern in a smaller more informal group. Arrange to have "lunch & learn" meetings with the staff so you can discuss the policy in a more casual setting.

Understanding the policy

This step is as important, if not more important then all the other steps. You can be as thorough as can be in performing your risk assessment, and go through the most vigorous testing and modifying your policy, but if no one understands what the policy means, its importance, and what their role is in it, then you will have accomplished very little.

Every user must understand that the responsibility of IT security does not end at the doors of the IT staff. It is everyone's responsibility to be aware of threats, the impact of the threats, and what needs to be done to avoid them. When you are meeting with the staff, cite specific examples of threats and their associated impacts. Make it a point to let them know that your door is always open for questions or concerns as it applies to the policy. It is important that they know when in doubt, they should come to you and ask, remember, there is no such thing as a stupid question. Have them leave your meeting with a strong comprehension of the policy, and knowing its importance.

Every Users Responsibility

In addition to every user's normal role in the organization, it is also their responsibility to understand and enforce the IT policy. As I have stated repeatedly throughout this paper, it is not only up to the IT professional to ensure a secure IT infrastructure. Every user's understanding of the policy is another building block in the overall security structure. All it takes is one person to make your infrastructure vulnerable to attack or intrusion. The excuse "I didn't know I should or shouldn't have done that" is something that you never want to hear.

Practice what you preach

It is important that you as the IT professional practice what you preach. Once a policy is set, no one should ever consider himself or herself above it, including the person or persons who wrote it. Make sure that you follow the rules and guidelines that you yourself help create. How embarrassing would it be to have to request funds to recover data from your crashed hard drive because you weren't storing your data on the network, as it states in the policy that you helped write?

Conclusion

Developing, and implementing an effective IT policy is an always evolving process. You will need to revise your policy as new threats, and methods for abuse rear their heads. It is important to remember that any policy is only as effective, as it is understood.

References

Computer Security Institute "2003 CSI/FBI Computer rime and Security Survey" (29 May 2003)
URL: http://i.cmpnet.com/gocsi/db_area/pdfs/fbi/FBI2003.pdf (21, Feb 2004)

"How to Develop a Network Security Policy: An Overview of Internetworking Site Security"
URL: http://wwws.sun.com/software/whitepapers/wp-security-devsecpolicy/

SANS Institutes, Basic Security Policy, Security Essentials, Network Security, Section 1.2

Mcgovern, Mark . "Best Practices – Opening Eyes: Building Company – Wide IT Security Awareness" (July 2002)
URL: http://www.sqmmagazine.com/issues/2002-03/itsec.html (22, Feb 2004)

Palmer, Ian. "Email abuse and Misuse"
URL: http://www.insight-mag.com/insight/03/08/col-5-pt-1-WorkForce.asp (22, Feb 2004)

Baskervulle, Richard and Spionen, Mikko. "An Information Security Meta-Policy for Emergent Organizations"
URL: http://www.oasis.oulu.fi/publications/lim150502-ms.pdf (23, Feb 2004)

Gaudin, Sharon. "Employee Abuse of Internet Rampant" (24, Apr 2002)
URL: http://www.internetnews.com/dev-news/article.php/1015141 (23, Feb 2004)

Mitnick, Kevin D. The Art of Deception. Indianapolis: Robert Ipsen, 2002

Last Updated: July 28th, 2017

Upcoming Training

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
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
Virginia Beach 2017 - SEC401: Security Essentials Bootcamp Style	Virginia Beach, VA	Aug 21, 2017 - Aug 26, 2017	vLive
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
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
Mentor Session - SEC401	Ventura, CA	Sep 11, 2017 - Oct 12, 2017	Mentor
Community SANS Albany SEC401	Albany, NY	Sep 11, 2017 - Sep 16, 2017	Community SANS
Community SANS Dallas SEC401	Dallas, TX	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Columbia SEC401	Columbia, MD	Sep 18, 2017 - Sep 23, 2017	Community SANS
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
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 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
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
Mentor Session - SEC401	Arlington, VA	Oct 04, 2017 - Nov 15, 2017	Mentor
SANS October Singapore 2017	Singapore, Singapore	Oct 09, 2017 - Oct 28, 2017	Live Event
Community SANS Indianapolis SEC401	Indianapolis, IN	Oct 09, 2017 - Oct 14, 2017	Community SANS