The Seven P's of Computer Use Policies

During the early 1990's, Thomas Jerry Scott and his good and brilliant friend, Richard Voss, spent over a year doing academic research on how to develop a Computer Use Policiy for individuals in organizations and academic institutions. The goal of the research was to find "a lowest common denominator" for what a computer security policy should be.

During the process, over 200 actual computer use policies were discovered, analyzed, and quantified. The research led to the development of "***The Seven 'P's' Model for Computer Use Policy Development***". Seven academic papers and one chapter of a book on Computer Security were published, as well as over 10 papers presented at academic computer and business conferences.

This note is a short synopsis of their main findings. It is provided for you to help you develop better policies for your users.

The "7 P's" were all items important in the successful development of a Computer Use Policy. The "7 P's" in order of importance were:

1. *Participation*

We found that having a committed, broad representation of people is the single, most important ingredient for a successful policy. Without broad participation, a policy will have things that many "did not buy off on" and will fail or be sabotaged.

2. *Philosophy*

The Philosophy issue revolves around two questions:

1. ***Do we reflect current activities?*** or

2. ***Do we shape the computer oriented behavior of our users in our organization?***

In a military environment, we should shape our organization's behavior, but in a commercial environment, we will often reflect behavior. The reflection might be the case when an organization is driven by some big sellers, who have particular habits and are responsible for much of the organizational profit.

3. *Partitioning*

A policy must not be a monolithic document! In most policy manuals, three layers are mentioned. These are:

1. ***Policy Statements or Goals***

These are your top level items. They are vague and not concerned with hardware or methodology. A goal or Statement normally refers in the broadest terms to what people can do and cannot do. An example of a goal would be:

Users can surf the web for one hour per day, but their web surfing must not harm our company networks and must not bring the company name into disrepute or cause prosecution.

Normally, a group of computer security experts can get high level management to "sign off" on the overall goals or statements.

2. ***Standards for Achieving the Goals***

A Standard defines how, again in broad terms, how the Policy Statement will be achieved. It normally defines the hardware and logistical procedures needed to accomplish the Goal. For example, in the above Goal, the Standard might say that "Firewalls, Routers, and Intrusion Detection Devices will be used to protect our users and our networks."

Normally, the network and security personnel work to determine the overall security design and mainstay components. When they have figure out these items, they usually report back to higher level management, which normally just signs off on the Standard. Higher-level management wants to know the big details, but not all the intricacies, such as why "Real Secure is better than Entercept" or why "Checkpoint was chosen over Cisco PIX".

3. ***Procedures to Achieve the Standard***

The Procedures section of a Policy contains such nitty-gritty details as firewall rules, router ACL lists, Web Server and Operating System auditing setup details, and IDS signatures.

4. *Privacy*

A successful policy must define what levels of privacy can be expected, as well as what is not considered private by the company or institution. Users need to know this, so they can behave properly and not incriminate themselves through such items as sending emails to others, while thinking emails are private.

5. *Persnickety*

For both Richard Voss and Thomas Jerry Scott, this "P" word conjured up references to elementary school teachers they had in their early development. The Persnickety component defines the level of detail the Computer Policy will contain.

If you make your policy too precise, it will become like legalese and not be readable. On the other hand, if you make it too vague, there will be violations that "slip through the cracks." Normally, a company has some styles it uses to communicate with employees. These should be used.

6. *Phog-phactor*

One of the first rules of successful writing is "***know your audience.***" We found that many of the policy writers were unaware of this rule.

In our research, we ran some word study and readability tests on our policies. We then averaged the readability levels for the policies.

Briefly, a readability level of 9 means that you can understand what you are reading if you have completed 9 years of school, i.e., have completed your freshman year at high school.

We found that the average readability level of our 200 analyzed policies was 19.7. We also found that the 25th percentile score was 17.8. This means that 75% of the analyzed policies had readability levels higher than 17.8. Wow!

Since over 100 of the 200 policies were from academic institutions, this meant that on average, only those at the PhD level could understand the average policy.

One of the real challenges in developing a policy is to say what you have to say in words that the intended audience will understand.

7. *Publication*

The last item was especially important to my colleague, Richard Voss, who passed the bar in Nebraska and always looked at our results with a legal mindset. In legal terms, "Publication" refers to how you notify your employees of their regulations.

We found that many groups went to great detail to publish policies, but assumed that everyone would just read them. How many beginning employees do you know who have read the company's computer security policy?

Normally, you achieve correct publication results by giving everyone a copy of the policy, and in addition, making them sign off that they have read it and understood it. This is challenging, but for a policy to be successful, people need to know it and understand it.