

# Introduction to Security Policies, Part One: An Overview of Policies

*Charl van der Walt* 2001-08-27

## Introduction to Security Policies, Part One: An Overview of Policies

by *Charl van der Walt*

last updated August 27, 2001

---

### Introduction

This is the first in a series of four articles devoted to discussing about how information security policies can be used as an active part of an organization's efforts to protect its valuable information assets. In a world that is essentially technology driven; where the latest IIS exploit is countered with a mad rush to install the relevant patch and where the number of different operating systems in a network exceeds the number of hairs on the security administrator's head that haven't turned gray, policies give us an opportunity to change the pace, slow things down and play the game on our own terms. Policies allow organizations to set practices and procedures in place that will reduce the likelihood of an attack or an incident and will minimize the damage caused that such an incident can cause, should one occur.

Many people see policies as an afterthought; a tasty dressing to be added to a veritable technology-salad of firewalls, virus scanners and VPNs, all lightly sprinkled with just a touch of IDS. This is wrong. In this series I'll attempt to explain why policies should be the basis of a comprehensive Information Security strategy, and how policies can be an effective, practical part of your digital defense systems.

### What is a Policy?

The nicest definition for 'policy' that I could find is from the American Heritage Dictionary of the English language. It reads:

"A plan or course of action, as of a government, political party, or business, intended to influence and determine decisions, actions, and other matters"

In practical security terms, I define a policy as a published document (or set of documents) in which the organization's philosophy, strategy, policies and practices with regard to confidentiality, integrity and availability of information and information systems are laid out.

Thus, a policy is a set of mechanisms by means of which your information security objectives can be defined and attained. Let's take a moment to briefly examine each of these concepts.

First, we have the information security objectives:

- **Confidentiality** is about ensuring that only the people who are authorized to have access to information are able to do so. It's about keeping valuable information only in the hands of those people who are intended to see it.
- **Integrity** is about maintaining the value and the state of information, which means that it is protected from unauthorized modification. Information only has value if we know that it's correct. A major objective of information security policies is thus to ensure that information is not modified or destroyed or subverted in any way.
- **Availability** is about ensuring that information and information systems are available and operational when they are needed. A major objective of an information security policy must be to ensure that information is always available to support critical business processing.

These objectives are globally recognized as being characteristic of any secure system.

Having broadly defined the reasons for implementing a security policy, we can now discuss the mechanisms through which these objectives can be achieved, namely:

## Philosophy

This is the organization's approach towards information security, the framework, the guiding principles of the information security strategy. The security philosophy is a big umbrella under which all other security mechanisms should fall. It will explain to future generations why you did what you did.

## Strategy

The strategy is the plan or the project plan of the security philosophy. A measurable plan detailing how the organization intends to achieve the objectives that are laid out, either implicitly or explicitly, within the framework of the philosophy.

## Policies

Policies are simply rules. They're the dos and the don'ts of information security, again, within the framework of the philosophy.

## **Practices**

Practices simply define the how of the organization's policy. They are a practical guide regarding what to do and how to do it.

In the sections that follow I'll be examining each of these mechanisms more closely.

## **In Praise of Policies: What Benefits Do Policies Offer?**

In the previous section we covered briefly what a policy is and, more specifically, what an information security policy is. From this brief description it should already be clear that, when it comes to policies, I mean business. And in IT this usually translates to a sizeable investment in time, money and human resources. Don't kid yourself; effective policies are no quick fix. The question on everyone's lips has got to be: "Yes, but what can I do with a policy that I can't do with Snort 1.7 on my favorite Bastion Linux install?" Here are some of the things policies will do for you that you'll struggle to achieve with technology.

## **The Boss Can Do It**

Most technological controls are the responsibility of the IS manager, the network administrator or some poor sod who didn't get her leave application forms in on time. Policy, on the other hand, is the responsibility of upper management. This thinking is consistent with company law in most countries that says it's the responsibility of the directors of a company to protect its assets on behalf of the shareholders. As such, the development of a policy includes the ancillary benefit of making upper management aware of and involved in information security. This should make it a higher organizational priority, which can only increase the level of security throughout the company.

## **They Provide a Paper Trail in Cases of Due Diligence**

In some industries your company may have legal obligations with respect to the integrity and confidentiality of certain information. In many cases the only way you can prove due diligence in this regard is by referring to your published policies. Because policy reflects the philosophy and strategy of your company's management it is fair proof of the company's intention

regarding information security. Interestingly, an audit against a security standard works on exactly this principle of 'intention'.

### **They Exemplify an Organization's Commitment to Security**

Because a policy is typically published, and because it represents executive decision, a policy may be just what is needed to convince that potential client / merger partner / investor exactly how clever you really are. Increasingly companies are requesting proof of sufficient levels of security from the parties they link to do business with. Once again, a security policy is exactly the place to start.

### **Practical Benefits of Security Policies**

OK, so much for the soft and fuzzy stuff. We said policies can play a practical role in securing your information assets. Here's how.

### **They Form a Benchmark for Progress Measurement**

Policy reflects the philosophy and strategy of management with regard to information security. As such it is the perfect standard against which technology and other security mechanisms can be measured. For example, if you want to know whether your brand new "Hack 'em Back" ultra firewall (performance tested by Russian cosmonauts on Mir) was really worth the price of a small Caribbean island, then check whether it's implementing the controls stipulated in the policy. Similarly, to determine whether the new IT manager is effectively investing her IT security budget, measure her progress against the policy. And here's the best part: if the policies are correctly formulated and carefully integrated into your employment contracts, then any transgressions against the policy, such as surfing porn on the company's network, can be punished according to a pre-established agreement that the employee has signed off on. An information security policy thus serves as a measure by which responsible behavior can be tested and suitably punished.

### **They help ensure consistency**

The biggest challenge facing security managers today is not how to negotiate a 512 bit RSA public key exchange using Diffie-Hellman and self-signed certificates (everyone can do that these days). No, the challenge is ensuring that the sysadmin in the Tahiti branch gets off the

beach in time to load the patch for the IIS Unicode exploit on the web server and avoid yet another embarrassing defacement on [www.tahiti\\_branch\\_of\\_my\\_respectable\\_company.com](http://www.tahiti_branch_of_my_respectable_company.com). A well-implemented policy helps to ensure consistency in your security systems by giving a directive and clearly assigning responsibility and, equally important, by stipulating the consequences of failing to fulfill those responsibilities.

### **They Serve as a Guide to Information Security**

A well-designed policy can become an IT administrator's Bible. Sadly, not everyone who will ever attach a computer to your network understands the threat of TCP sequence number guessing attacks against OpenBSD. Fortunately, your IP network security policy will ensure that machines are always installed in a part of the network that offers a level of security appropriate to the role of the machine and the information it hosts.

### **They're Define Acceptable Use**

People can be either the strongest or the weakest link in any information security system. Although training, positive enforcement and technology can all play a role in making people a part of the solution and not part of the problem, in the end there's nothing like a big stick for bringing people over to your way of thinking. An integrated policy can be just such a stick in that it serves as a measure of performance according to which responsible people can be measured and potentially disciplined. By clearly defining what can and cannot be done by users, by pre-establishing security standards, and by ensuring that all users are educated to these standards, the company places the onus of responsibility on users who can no longer plead 'ignorant' in case of transgression of the policy.

### **They Give Security Staff the Backing of Management**

The objectives of information security are often at odds with the desires of system users. How many times has a user thanked you for disabling Active X in her browser and blocking access to *Napster*? Often security staff face resentment and opposition from people in more senior positions to themselves. The policy, as a directive from top management, empowers security staff to enforce decisions that may not be popular amongst system users. Armed with a policy your security administrators can do their jobs without having to continuously justify themselves.

## **Policy Power - Making Policies Work**

OK, OK you're sold. You've seen the light and decided to seriously undertake the implementation of information security policies in your own organization. But how? In the sections that follow I'll try to share with you some of the tricks of the security policy trade.

## **Defining the Objectives**

### **What Are the Policies Actually Protecting?**

Before making decisions regarding the Information Security strategy (long or short term) organizations need to have a sound understanding of their unique risk profile. Risk consists of a combination of information resources that have value and vulnerabilities that are exploitable. The magnitude of the risk is the product of the value of the information and the degree to which the vulnerability can be exploited.

As long as the organization has information that has value that information - and by extension, the organization - will be subject to risk. The function of any information security control mechanism (technical or procedural) is to restrict that risk to an acceptable level. This is also true for policies. Policies are a risk-control mechanism and must therefore be designed and developed in response to real and specific risks. Thus, a comprehensive risk assessment exercise must be the first phase of the policy development process. The risk assessment should identify the weakest areas of the system and can be used to define specific objectives.

Of course there is also a sheet-bombing approach to policies and generic policy documents are freely available on the Internet and from various commercial resources. Although there are a number of issues that can be dealt with in a generic manner one should be very careful of this approach. A policy that says too much is no better than a policy that says nothing at all. Organizations must be prepared to enforce every stipulation your policy makes (I'll say more about this later in this paper) so policies must be focused and specific.

Security administrators need to define objectives for their particular organization, based on the value of that information and the specific risks that information faces.

## **Setting the Stage**

### **Next Time: Creating an Environment that Supports Security Objectives**

Policies in themselves are ineffective and their potential to be effective is directly proportional to the support they receive from the power structures of the organization. Thus there is a flow of authority that stems from upper management and expresses itself in the implementation of the stipulations of the policies. For this flow to happen certain fundamental changes may have to be made to the structures and culture of your organization. The bigger the organization, the more important these changes become. In the next article in this series, we will discuss some of the organizational conditions that are necessary in order to ensure that information security policies are effective.

To read **Introduction to Security Policies, Part Two: Creating a Supportive Environment**, click [here](#).

[Privacy Statement](#)

Copyright 2006, SecurityFocus