

Introduction to Security Policies, Part Three: Structuring Security Policies

Charl van der Walt 2001-10-09

Introduction to Security Policies, Part Three: Structuring Security Policies

by *Charl van der Walt*

last updated October 9, 2001

This is the third in a four-part overview of security policies. In the [first article](#), we looked at what policies are and what they can achieve. In the [second article](#), we looked at the organizational support required to implement security policies successfully. In this installment, we shall discuss how to develop and structure a security policy.

Structuring your policy: How do we put it all together?

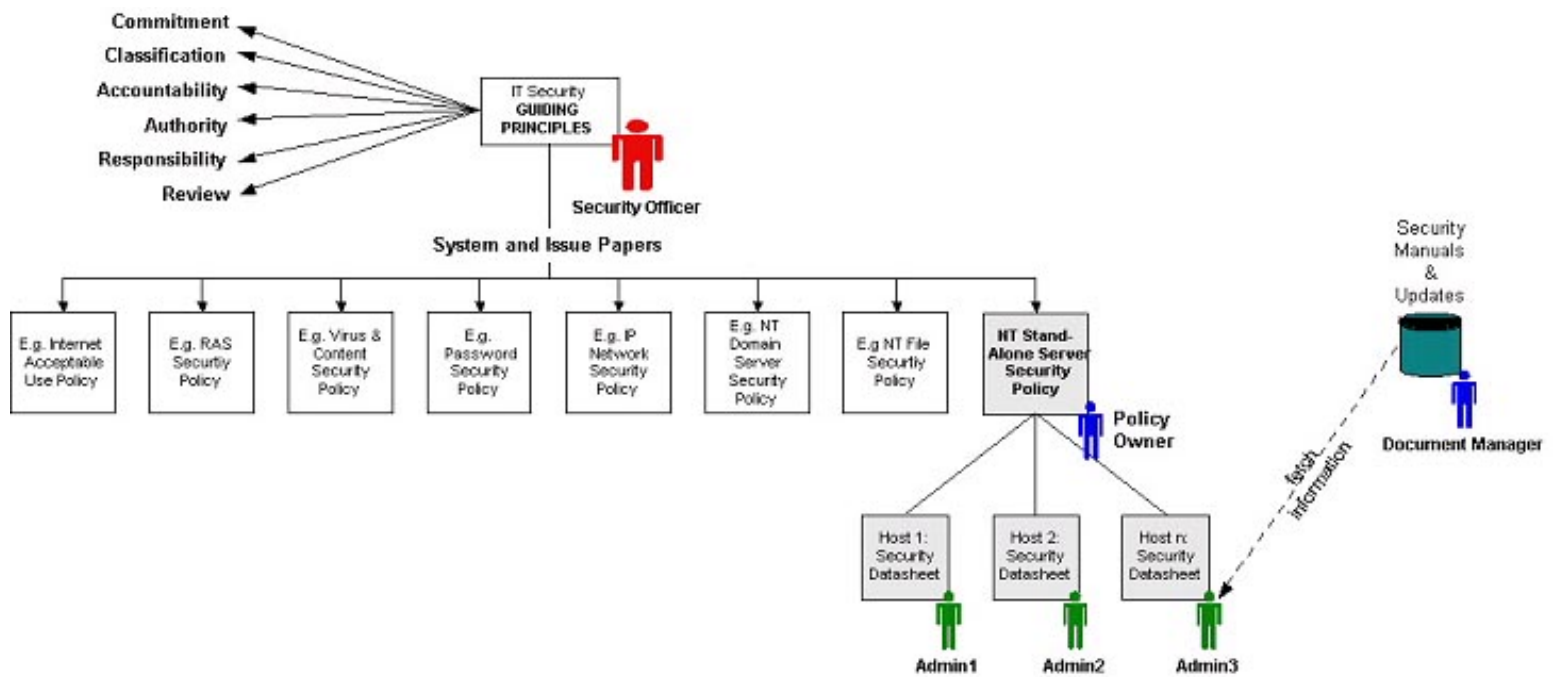
An effective classification system can help to make your security policies simpler and easier to develop; however, if they are to be implemented in a large organization that employs a diversity of technologies, the development of policies will still require a lot of work. It is essential that the policies be structured and packaged in such a way that they are as light as possible, without missing any important issues. By "light" I mean that they should be:

- Light, not weighing. Not using too many trees.
- Simple and practical.
- Easy to manage and maintain.
- Easy to access by people seeking specific information.

To meet these requirements, I typically recommend that a policy be split into a number of smaller policies and that these be arranged in a hierarchical fashion. The 'smaller' policies I refer to are known and position papers and they contain specific policies regarding (yes, you guessed it) specific issues and specific systems. Because each one of these position papers is focused, it can be kept short and practical, can be written by a specialist and can easily be modified or updated without having any effect on the rest of the policy.

The Security Framework Document

Although each position paper may be written by a different author - typically a specialist in that field - we still want all the papers to subscribe to some fundamental principles. These principles (what I call the security philosophy) should be laid out in a single document known as the Security Framework paper. This paper, along with the classification system, creates a framework of values and principles upon which each other document should be based. It can be considered an overview or an outline of the Policy as a whole. The Security Framework also forms a kind of default policy that can be referred to whenever there is doubt or in cases where there is no current policy paper relevant to a particular system. This concept is depicted in the following diagram:



Let's examine each element of this framework in turn:

The Security Framework paper defines a minimum set of organizational security requirements that is applicable to all management, staff and external consultants. The document defines a set of concepts and principles that are designed to ensure the protection of all information assets, and the technologies used to store and transmit them. No decisions regarding the security of information and information technology (IT) should be made without careful consideration of, and due compliance with, the concepts and principles described in the Security Framework document.

The Security Framework document should cover at least the following important points:

1. The value of information and the organization's commitment to information security.
2. The classification system, which was discussed in the [second article in this series](#).
3. The principle of accountability that states clearly that users and administrators will be held accountable for behavior that impacts the security of information.
4. The designation of authority to the Security Officer and security-related people in the organization as is appropriate.
5. The principle of individual responsibility of all system users for the security of information resources.
6. The organization's approach to security reviews; for example, how often they will take place, who will perform them, etc.

The function and responsibilities of the Security Officer (SO) have already been covered in some detail in the [second article](#) in this series. The SO assumes ultimate responsibility for security in the organization. It is his or her job to guide, advise and review the organization's security policies and procedures. The Security Framework document thus usually falls under the SO's jurisdiction, as does the management and distribution of the various position papers. In a large organization, the SO may have a dedicated Document Manager on her team, someone whose specific responsibility it is to ensure that all the policy documents are kept current, that changes are properly controlled and that users have free and easy access to all necessary security information.

Position Papers

Position papers are written to address the a specific aspect of the security policy such as the security of some specific technology, or security in a particular situation. For example, one might have a position paper covering the secure configuration of Windows 2000 member servers that are connected to the Internet, as well one describing the process to be followed in the event of a breach of security measures (commonly known as a security incident.)

The position papers address these specific security issues in a way that is concise, practical and easy to understand. They should also address the issues in ways that are directly relevant to the organization. Because these papers are so focused they can be kept short and to the point. They are easily modified and can be written by someone who is an expert in that particular field. Exactly what topics should be covered varies from organization to organization: I make some comments on this question in the Policy Content section a little later in this article.

Policy Owner

The Policy Owner is the person responsible for the maintenance and integrity of a given policy document. No changes may be made to a document without the express permission of the Policy Owner. The name of the Policy Owner must be clearly displayed on the document and the document should always be dated and signed by the owner. Having a Policy Owner ensures consistency in policy and accountability for the validity and efficacy of that particular aspect of the policy.

Security Datasheets

I typically recommend that each IT system have a security datasheet. The datasheet document lists specific settings and parameters that ensure the security of the system. Whereas the Security Framework document and the various position papers refer to policy in general, the datasheet introduces the details that should be applied for each system. Each system or host should have a datasheet that is managed by the system owner and is subject to the principles of this document and the System Paper.

It is the responsibility of information and technology owners and users to obtain the relevant papers from the SO or the STF and ensure that the standards defined therein are correctly implemented on the systems they control.

Technical Guides

Technical guides are another set of useful documents, although they are not actually policies. Technical guides outline the implementation, operation, configuration and administration of specific systems. They can be bought off-the-shelf or the organization can commission experts to write them. They can be stored along with the policies and referred to by the position papers. For example, instead of using a position paper to describe exactly how Solaris-based Apache Web servers should be configured, the organization can write or even purchase a guide that covers exactly that. Again, this contributes to the modular nature of security policies and makes them both easier to use and easier to manage.

System Owner

In the section about classification in the second article in this series, we referred to the concept of ownership. The System Owner is the person responsible for the technical management of a given IT system. It is his or her responsibility to ensure that the specifications of the Security Framework document and the relevant position papers are implemented and maintained. It is also the System Owner's responsibility to decide on the classification of the system, should it differ from the default. The name of the System Owner is given in the datasheet for each system and should clearly displayed whenever a user accesses the system and on or near the system itself where it can easily be seen.

Policy Content

Now that the framework of the security policy is in place, readers may be wondering just what they should say. There is no set answer for this question, as it depends on the organization in question. The policies must be based on the real requirements identified by the security risk assessment that the organization should have performed. But everyone loves a shortcut, so here are two:

1) What the Position Papers Should Say

Scope - precisely what issue, organizational unit or technological system that the paper cover.

Validity - each policy should have a limited lifespan and be reviewed on a regular basis.

Ownership - a name and contact details for the 'owner' of the document, as described earlier in this paper.

Responsibilities - a description of who is responsible for which elements of the security of the system or issue being covered. This is important if one wants to enforce accountability.

Supporting Documentation - a reference to other documents higher or lower in the policy structure, for example, the Security Framework document or a specific Technical Guide.

Position Statement - what you actually want to say about the issue (kind of the hard part.)

Review - whether, when and how security reviews will be performed on the systems in question.

Compliance - a statement regarding the consequences of non-compliance with the policy.

2) Policies for Free

There are a number of good examples of policies to be found on the Web, both for free and at a price. One excellent resource for position papers is Mr. Charles Cresson Woods' comprehensive book - "Information Security Policies Made Easy", which is available from [Baseline Software](#) . Although my feeling is that Mr. Cresson Woods' policies are (for the most part) too generic, his book can give you an idea of what should be covered and there definitely are some policies that can be used. The book comes with a CD that has the policies in electronic format for easy copy-and-pasting.

What Topics should the Position Papers Cover?

Here's a list of position papers that should exist for most organizations:

- Physical Security
- Network Security
- Access Control
- Authentication
- Encryption
- Key Management
- Compliance
- Auditing and Review
- Security Awareness
- Incident Response & Disaster Contingency Plan
- Acceptable Use Policy
- Software Security

Assessing Policies

Once an organization has a system of security policies in place, it will be necessary to determine the efficacy of the policies within the context of the organization. The proper way to do this is, of course, via another risk assessment exercise, thus completing the security cycle. However, it may be possible to properly assess the policies without having to go through the entire risk assessment process. The following is a list of simple questions security personnel can use to assess how effective the policy will be for their particular organization. These are typically also the questions that auditors and security analysts will be asking themselves as they review your security mechanisms.

1. Does the policy have a clearly defined scope? Is it clear to which system and which people the policy is applicable?
2. Is the policy comprehensive in terms of the defined scope it means to address? Are all systems and issues sufficiently covered?
3. Does the policy clearly define responsibilities? Is it clear to the end-user, the line-manager and the various administrators exactly what his or her responsibilities are? Is it clear who is responsible for various aspects of security?
4. Is the policy enforceable? Can it be applied in a concrete manner so that the compliance is measurable?
5. Is the policy adaptable? Can it be easily changed to address new risks and new technologies?
6. Is the policy having its desired effects?
7. Is the policy universally known and understood within the organization? Is the policy well distributed, is there an awareness of the policy and is its content understood?
8. Does the policy comply with law and with duties to third parties? Is the organization fulfilling its statutory obligations?

Global Best Practice: Measuring Policies Against International Standards.

At least one good reason for an organization to have security policies is to display that it is taking all reasonable steps to ensure the confidentiality and integrity of its information assets. This is particularly important for publicly-listed companies, for companies in the process of mergers and acquisitions, and for companies seeking investors and business partnerships. As security becomes more of a public relations concern, large organizations will require their e-business partners to comply with a set of operating regulations that ensure that appropriate levels of security are maintained. For example, industry leaders like VISA have already begun this process with their partners.

What are "appropriate levels of security" then? These levels are often dictated by standard-setting organizations, such as [The International Organization for Standardization](#). A security standard contains a list of required controls that need to be in place in order to ensure appropriate levels of security. When an organization has effectively implemented the controls prescribed by the standard it can apply for certification of standard adherence or compliance from the standard's governing body. One standard that is frequently used in security circles is BS 7799. Issued by the [British Standards Institute \(BSI\)](#) in the United Kingdom, which has been incorporated into the ISO standard set. ISO 17799 comprises 137 control objectives that must be achieved before an organization can apply for certification to the standard.

Implemented properly, standards like ISO 17799 can significantly further an organization's IT security objectives, but readers should be aware that this is not the only available security standard today. It is important for an organization embarking on the long and hard (and expensive!) route to certification to understand what the envisaged security standard will offer them and their business partners in the long run.

If an organization is considering structuring your policies within the framework of a security standard like ISO 17799, here are some issues the it should consider addressing:

1) Recognition - If a major purpose of certification is to assure customers of the organization's security readiness, the certification chosen must be highly regarded by the target market. This is probably the single most important factor.

2) Focus - The various certification programs tend to focus on different aspects of IT security. For example, GMITS takes a business-oriented approach whilst ITSEC tends to focus on technology. A certification path needs to be chosen that is compatible with your organization's own security objectives.

3) Local presence - Apart from the standards body itself the process of certification typically requires the participation of two other parties - the process consultant who will lead you through to certification and the assessors who make the certification approval. You must determine if the correct people are available to be in your country or state to do this work. This is of course particularly important for the BSI standards.

4) Cost - The cost of the certification must be weighed up against the value it offers.

5) Endurance - The certification process should have long-term benefits that outweigh the costs. This means:

- The effects of the process should be practically tangible (the systems should be more secure afterward)
- The process should not have to be repeated too often.

6) Objectivity - It is generally not a good idea to be officially audited by companies that also sell security products. However, this is not a black-and-white issue and most security companies today offer both services and products successfully.

Conclusion

This concludes our discussion of designing and structuring security policies. In the next, and final, installment of this series devoted to developing effective security policies, we will walk through a couple of examples of security policies.

To read **Introduction to Security Policies, Part Four: A Sample Policy**, click [here](#).

Relevant Links

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

Charl van der Walt

Introduction to Security Policies, Part Two: Creating a Supportive Environment

Charl van der Walt

[Privacy Statement](#)

Copyright 2006, SecurityFocus