



astaro
internet security

Network Security Whitepaper

**Good Security Policy Ensures Payoff
from Your Security Technology
Investment**

Version: 1.00
Release date: June 2, 2004
Author: Alan Radding



Good Security Policy Ensures Payoff from Your Security Technology Investment

Astaro www.astaro.com info@astaro.com
3 New England Executive Park, Burlington MA, 01803 USA
Pfinztalstrasse 90, 76227 Karlsruhe, Germany

Table of Contents

Security breach! What am I supposed to do about it?	3
Why have a security policy?	3
Policy drives security investment	4
Establishing a baseline	4
Assigning responsibility.....	4
Risk mitigation strategy	5
Elements of an effective security policy.....	5
A process for creating an effective security policy.....	7
Gather information from existing tools.....	8
Recommendations	8
Conclusion: Security investment value is reduced without policy	9
About This White Paper's Sponsor: Astaro.....	9

Security breach! What am I supposed to do about it?

If somebody in your organization discovers a breach of security does he or she know what to do? Who is responsible for preventing security breaches in the first place? Who fixes the damage? Who is held accountable?

Why have a security policy?

The lack of an effective security policy can frequently undermine even the best security tools. If users are not told that it is a violation of the corporate security policy to bring in code from the outside, then they will bring it in, bypassing your gateway-based anti-virus defense. If there is no corporate security policy prohibiting users from visiting inappropriate sites, then the best content filtering software will be of little help. Users will do bad things, but nobody will have the authority to stop them.

A security policy performs several functions that help ensure the effectiveness of whatever security strategy the organization pursues. Specifically, it:

- Identifies threats—names the types of activities, behaviors, and events that constitute a threat to the organization
- Defines acceptable security practices—explicitly describes from a security standpoint how an employee should use corporate information systems
- Mandates defensive actions—defines the kinds of steps that must be taken to counter the named threats
- Establishes roles and responsibilities—assigns security tasks and accountability to groups and individuals for failures to take appropriate actions in response to threats, and for actual breaches and attacks
- Guides implementation and investments—enables the organization to effectively prioritize and budget for the implementation of various components of the security strategy

Good security practices alone mandate the development and widespread adoption of a security policy. But now the government will increasingly force your hand as well. Government regulations, from the Patriot Act, to Sarbanes Oxley, to HIPAA and many others, often include a security mandate that holds the organization responsible for ensuring the integrity and the privacy of the data and the integrity of the systems that manage the data. Failure to comply with these mandates can result in financial penalties and even land executives in jail.

Beyond the government, other stakeholders have a strong interest in the security policy. Employees want to have clear guidance in the face of incessant news about virus attacks, hacking, and other security breaches. Customers need reassurance that the organization is

committed to protecting their data and privacy. A good security policy helps to address all these concerns.

Policy drives security investment

A security policy provides the foundation for the organization's security strategy and drives the investment in security tools. If you haven't identified access to inappropriate sites as unacceptable corporate behavior, then you're not likely to think about investing in content filtering. If hackers and intruders aren't deemed a threat, why bother with a firewall? If a virus attack doesn't worry you, then why install anti-virus software?

Of course, no serious organization today would ignore virus attacks, hackers, employee surfing of illicit websites, or other common threats. Still, it is difficult to plan and budget for security investments in a responsible way without a documented security policy that identifies and prioritizes the likely threats and assigns responsibility. Similarly, without a security policy that has been communicated to everybody in the organization, it is difficult to make people responsible for security tasks, or to hold accountable those responsible when security is breached.

Establishing a baseline

Although experts often recommend developing the security policy before making any investment in security tools, such an approach is unrealistic at this point. Most organizations already have a few security tools in place. However, this is no reason to not develop a formal security policy. On the contrary, these tools can help in the development of the policy, particularly by identifying and quantifying threats and risks.

The reporting provided by these tools is instrumental in establishing a security baseline from which you can assess the effectiveness of your security policy and strategy in the future.

Assigning responsibility

There is a business adage that if a job is not someone's specific responsibility it won't get done. The security policy is also central to assigning responsibility. It identifies the people specifically charged with carrying out the security policy. The security policy assigns certain tasks or roles to specific individuals and clearly establishes the responsibility of every individual for behavior that jeopardizes security. Specific roles may include:

- Security manager or administrator—the person with overall responsibility for coordinating, directing, and managing security efforts on a daily basis
- Network security administrator—the person responsible for security threats that come in over the corporate network

Obstacles to Effective Security

Lack of top executive involvement and support
Lack of a security policy
Failure to educate employees on security
Lack of sufficient budget
Failure to assign responsibility
Failure to communicate and enforce security policy

- System security administrator—the person responsible for desktop and server security
- Data security administrator—often a database administrator, responsible for security of the production databases, data warehouse, and data marts
- Privacy administrator—often from the HR department, responsible for ensuring the privacy of personal information

In smaller organizations all or some these roles may be combined. In very large organizations or decentralized organizations multiple people may have these roles. The important thing is that security responsibility must be specifically assigned. In addition, a top executive must have overall responsibility for security and be prepared to demand accountability. If top management is not fully involved in the creation of the security policy and does not stand behind it completely, it will not work.

Risk mitigation strategy

The security policy also describes at a high level the organization's defense and risk mitigation strategy—how it intends to achieve the organization's security objectives. In effect, it lays out the security plan at a high level, typically leaving the specific implementation details to those charged with implementing the security program.

The organization can then use the plan as described in the security policy as a guide to the acquisition of appropriate security tools and products. At this point, it is important to avoid getting bogged down in quibbling over details of the plan—paralysis by analysis. Rather than leave the organization vulnerable from a security standpoint while policies or roles are being hashed out, the organization is better off immediately implementing the top priorities agreed upon. It can always revise and expand the security policy later.

Elements of an effective security policy

Security policies vary widely in scope and detail. Whether the security policy is a two-page document or a 50-page handbook, they all include some basic components. The following table describes the basic components of a security plan and the purpose.

Components	Purpose
Objectives	Declares the importance of security and the reasons for it Establishes exclusive corporate rights to data, networks, systems and the corporation's interest in defining and enforcing acceptable behavior
Security policy team	Defines the policy team, typically headed by the information systems group but

Implementation	<p>including people from other departments (HR, legal, key business units) Ensures buy-in across the entire organization Must have a top executive on board</p>
Communication/documentation	<p>Describes the security strategy at a high level Establishes threat priorities Describes response to attacks, threats, breaches, and violations Describes acceptable behavior</p> <p>Ensures that everyone is aware of the policy and his or her role in security Must be a published document widely circulated to every person in the organization</p>
Education	<p>Everyone must be educated to the contents of the policy and its implications for each individual - circulating the policy is NOT enough Specifies acceptable behavior (e.g., not leaving systems logged onto the network) Calls for periodic re-education</p>
Enforcement	<p>Policy without enforcement is meaningless (studies show that only 30% of companies actually enforce their usage policies) Specifies monitoring and measurement Specifies reporting Specifies penalties for violations and failures</p>
Review	<p>The policy must be periodically reviewed and updated due to changes in the business, technology, people, and threats</p>

The security policy may be published on paper or posted on the corporate network or intranet. One way or another, it must be disseminated to every individual. Some organizations require that employees sign a document attesting that they have read the security policy. Even then, ongoing education is a must. The goal is to raise the level of

security consciousness to the point where everyone is always aware of the security implications of everything they do.

A process for creating an effective security policy

Creating an effective security policy requires does not require technical security expertise. Security consultants can provide such expertise when it comes time to implement the policy. Instead, the policy development team must bring strong knowledge of the business and its various processes. It must be able to recognize threats and vulnerabilities at the business level.

Development of the security policy involves a 5-step process:

1. Set objectives—the team specifies the goal of the security policy and explains why security is important to the organization. It also should make it clear in the most straightforward terms that the systems, networks, and data are valuable corporate assets that are to be used for company business only (unless there is a valid exception).
2. Prioritize threats—the team identifies key threats or types of threats and specifies the level of risk each presents. It determine how much security is appropriate for each threat given its likelihood and level of risk. This is a process of balancing risk and cost. The team may determine, for example, that virus attacks are a high priority given the amount of damage viruses can cause and the high cost of repair. Preventing access to certain websites, on the other hand, may be a lower priority.
3. Describe acceptable behavior—the security team must specifically define acceptable behavior. It must be specific enough to enable people to act upon it yet not be so detailed as to be confusing, overly complex, or to create unintended loopholes. Common sense should be your guide. [see sidebar, Sample Acceptable Behavior Statements]
4. Establish monitoring and measurement—a security policy without an enforcement component has little value. The team establishes the company's intention to monitor and measure usage of the information systems and networks for the purposes of enforcement of the security policy and accountability.
5. Define penalties—the team lays out guidelines for managers who must hold workers accountable for security policy violations. These guidelines should be reasonable and appropriate and, most importantly, realistic. No manager wants fire an otherwise good employee for inadvertently bringing a virus into the company. Similarly, if the company tolerates a certain amount of personal use of the telephone, it is unrealistic to prohibit all personal web surfing.

In addition, the security policy should establish a timeframe and a scope. It should specify when the policy takes effect, how long it is in effect (often, until further notice), and the scope of the policy (Does it extend to offsite system usage?).

Sample Acceptable Behavior Statements

- Access to company systems and data is restricted to authorized users in the performance of their assigned tasks only
- Every user must have a unique ID and password, and passwords must be changed every three months
- Users must turn off, shut down, or lock up systems at the end of each workday
- Employees are to report any type of security incident, unauthorized access, data theft or damage, or virus infection to the security team immediately upon discovery.

Gather information from existing tools

Since most organizations already deploy some security tools, a firewall and anti-virus software at the least, the policy team can use information gained from these tools to identify likely threats, assess the level of risk, and prioritize the threat.

Recommendations

Developing a security policy is one of those tasks that is easy to put off because it does not directly and immediately appear to contribute to the company's business objectives. Also, with most companies already having put in place some security defenses and some ad hoc, informal security policies, a written security policy may seem unnecessary at this point.

But a formal security policy is more important now than ever before, especially with today's heightened concerns about governance and compliance and with regulators becoming increasingly interested in security and privacy issues. Use the security policy to help guide the security team in implementing cost-effective security to meet the organization's security objectives.

To that end, we recommend:

- Develop a security policy now rather than later
- Relate the security policy to business objectives and strategies to bolster the case for security
- Secure top management buy-in and active involvement
- Keep the policy independent of implementation (don't specify specific products or implementations)
- Review and modify the policy regularly as the business, threats, technology, people, and risks change
- Confront sensitive issues upfront and directly, especially pornography and pirated material

- Pay attention to bulletin boards, discussion groups, and weblogs, which raise free speech issues that must be addressed
- Consider the policy's impact on workers, workflow, and processes (If security is perceived as a hindrance, people will undermine it.)
- Set appropriate penalties or they won't be enforced
- Educate, educate, educate at the outset and on an ongoing basis

Conclusion: Security investment value is reduced without policy

A security policy is key to maximizing the value from your security investment. It enables the organization to establish responsibility for security and hold people accountable for security failures. Without responsibility and accountability, all other security investments are undermined.

The security policy also guides smart security investments. It establishes investment priorities, alerting managers to the capabilities they need and when and where to deploy those capabilities.

Finally, the security policy lays the foundation for a security-conscious culture. People know the importance of security to the business, know what is expected of them, and know they will be held accountable.

About This White Paper's Sponsor: Astaro

The security policy will serve as a guide for helping you select the right security products to implement your security strategy. By identifying risks and setting priorities, it will help focus the security investment.

Selecting Astaro Security Linux is a smart investment in terms of both security protection and security policy development. Astaro Security Linux is the best-selling open source-based network security product and winner of numerous awards. A comprehensive solution, it delivers industry-leading capabilities in the areas of firewall, content filtering, virus protection, spam protection, and intrusion detection.

In addition, Astaro Security Linux can help in developing an effective security policy. It provides reports that show overall activity levels, the number of potential intrusions, the number of viruses, the quantities of spam received, and web usage. These reports can be used to establish security activity baselines and to set priorities.

Now in its fifth release, Astaro Security Linux is protecting 20,000 networks in more than 60 countries. In addition to its use as a primary security solution, many organizations that have deployed other security tool find it is highly effective and economical to augment their existing security solution with advanced functionality from Astaro, such as URL filtering.