

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

Charl van der Walt 2001-09-24

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

by Charl van der Walt

last updated September 24, 2001

As we concluded the [first article of this series](#), we pointed out that policies in themselves are ineffective; their effectiveness is directly proportional to the support they receive from the organization. Thus it is crucial that the organization be aware of the importance of security policies and create an environment in which security is given a high priority. The bigger the organization, the more important this support becomes. This article will go over a few of things that can be done to ensure that security policies given the full support of the management of the organization, which will thereby increase the efficacy of the policies.

Management support

I've touched on the importance of management buy-in a few times now already but it's worth stressing again. One of the biggest challenges facing security people is to convince management of the importance of their involvement in the process. Once again risk assessment and penetration testing can help with this. Without the buy-in of management at a high level the policy development process is unlikely to succeed.

Organizational structure

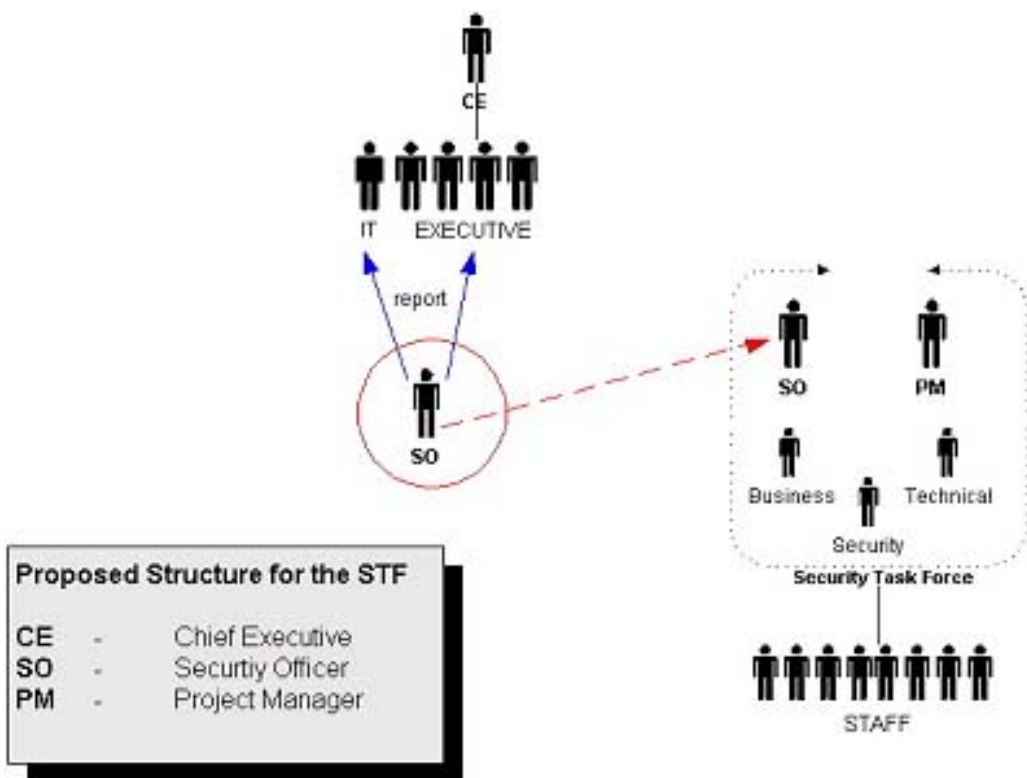
No matter what the size of the organization, a policy should always have an owner. While the titles or acronyms may vary from organization to organization, the roles, duties and obligations should be fairly consistent throughout. For the sake of this discussion, I will call this person the 'security officer' or 'SO'. It is the responsibility of the security officer to oversee the creation, distribution, and implementation of security policies. In this sense, the SO plays the role of intermediary between management and the user base. It's obvious then that the SO should report directly to the organization's highest level of control - the board of directors or even the chief executive.

Because the SO ultimately carries corporate responsibility for information security it is often

sensible for him or her to be a member of the board. In a small or medium organization the role of SO may not constitute a full portfolio but could simply be an added responsibility. However, no matter how small your organization, the SO role should be clearly assigned and the responsibilities precisely described. As owner of the policy the SO has a number of responsibilities including, but not limited to, the management and distribution of the security policy.

Typically the SO is responsible for aspects of security in the organization, not just issues relating to policy. It may be that the management structures in your organization have to be adjusted to make provisions for the new role. In large organizations that are still early in the security cycle we often propose the creation of a security team or task force (STF) to take responsibility for the security process. Such a team typically consists of the SO, a project manager (PM) and a collection of business, technology and security specialists. The functions of the STF include:

- Defining security strategy;
- Creating a mission statement and project plan; The investigation of a formal accreditation program (more on this later);
- Defining the corporate security policy;
- Defining system specific policies (more on this also);
- A user awareness program; and,
- The appoint of Security Auditors. The structure of the STF is depicted in the diagram below:



Financial Support

The security process will always require an investment in time, human resources and finance. Without sufficient financial commitment any security effort is bound to fail. The same is true for the policy development process.

In acquiring funds for the implementation of policies we once again see the value of a comprehensive risk assessment exercise. A properly implemented risk assessment should give a good indication of the risk to which your organization's information resources are exposed, the potential financial losses that may stem from any degradation of those resources may cause, and the role that policies can play in mitigating that risk. These indicators, combined with a fair understanding of the value of your information resources (possibly also gained from the assessment) should provide enough objective data to motivate and scope a financial investment in security.

A Culture for Security

A chain is only as strong as it's weakest link, and the weakest link in a security system is often the end user. Such problems are exemplified by a new generation of products that allow users to bypass "that pesky" firewall by subscribing to a service that tunnels TCP traffic over HTTP via a Java Applet that runs in any browser. I quote:

"ABC is a general-purpose tunnel that allows you to pass through that firewall. ABC works by mapping your network requests into web request to our server, so if you can read this page, you can use ABC! ? The uses for ABC are limited only by your imagination. It can pass anything that uses TCP!"

That means that even if your firewall allows only HTTP requests out, and those only via a proxy that expects user authentication, a clever user can still do whatever she wants on the Internet. If your users don't understand the value of your information assets and the risks that these kinds of technologies represent, then you'll be fighting a losing battle. You need to create a culture in your organization that is conducive to the implementation of security policies. I refer to this as "Selling Security" - and it's enough of a subject for an article on its own - but here are some strategies that administrators should consider in order to create an organizational culture that will place primacy on security:

1. User Education - Administrators can consider launching an internal advertising campaign explaining the value of the corporate information, the risks that it faces, the role of the policies and the responsibilities of the individual users. They may consider using a series of slogans like "Your password is you!"
2. Focus on managers - Management usually sets the tone for the workers underneath them and most passionately enforce the things they personally believe in. Convince the management of the need for security and half the struggle is won.
3. Be up front with staff - Employees are generally loyal towards the companies they work for, so being honest with staff about security and the impact it has on the organization will usually help to win people over to the security cause. One way to do this is to publish the results of security assessments and audits, or to play open cards about hacking and other security incidents.
4. Positive reinforcement - Because a well-designed policy allows for measurability, staff can now be rewarded for good security practice. Security administrators could consider the implementation of an incentive scheme per department that's based on the results of an annual security audit? Remember, a rule without punishment is just good advice?
5. Negative reinforcement - If the incentive of positive reinforcement does not instill a sense of

urgency, admins can consider going the other way. Firms may want to consider taking disciplinary action against staff for non-compliant or negligent behavior. Once again, policies introduce measurability and make this sort of action possible. They also give employees clear guidelines of acceptable behavior, and clearly spell out the consequences of breaching those guidelines.

6. Acceptance and Signoff - All staff should be made to sign a document stating their acceptance of the principles of the security policy. This forces staff to read and understand the policy and gives your organization legal recourse in the case of security breaches.

Using a Classification System

In developing the information security policies, security personnel will need to be able to distinguish between various groups of people, computers and information that have differing value and differing requirements in terms of security. This is a form of classifying information in terms of its accessibility to people within the organization. A statement like "Only authorized staff are permitted access to confidential data" isn't worth the disk segment its saved unless it is clearly stated who is "authorized" and what data is considered "confidential". This is no simple task: a large area of work has been done in the security field to answer exactly those two questions. This work has resulted in development of security "classification" systems - models by which information resources and people are assigned classification levels which are then used to describe what people will be allowed access to what resource classifications.

Formal Classification Systems

Let's briefly explore two such systems, just by way of example:

1. The Military Model [1]

In military circles, it is common for information to be classified into five levels:

- top secret
- secret
- confidential
- restricted
- unclassified

These levels form an ordering with top secret at the top, and unclassified at the bottom. Users are also assigned a classification, and the following rule is applied: "To have access to a document, the user must have a classification at the same level as, or higher than, that of the document." These levels are sometimes known as the rank of the information (or user).

Access to military information is also governed by the need- to- know principle, which places information in compartments. Compartments may extend across security levels, and information and users may belong (have access) to a number of compartments.

The full classification of both information and users is therefore defined by the pair [rank, compartments].

In the case of users, the [rank, compartments] pair is called the security clearance of the user.

2. The Bell-LaPadula model [1]

Bell-LaPadula is essentially a simplified version of the Military model and is designed to be slightly more user-friendly and appropriate to the commercial organizational environment. Bell LaPadula relies on the fact that there exists a partial ordering of security classifications/ clearances.

If $c(O)$ is the classification of the (data) object and $c(S)$ is the clearance of the (user) subject then two simple rules (known as "properties") apply.

1. The Simple Security Property (ss): A subject (S) may have read access to an object (O) only if $c(O) < c(S)$
2. The "*" Property (star): A subject (S) who has read access to an object (O) may have write access to another object (P) only if $c(O) < c(P)$

The first rule is fairly straightforward: no one may receive a piece of information unless their clearance is at least as high as the classification of the information they are accessing

The second rule states that information obtained from an object may only be passed to another object if the classification of the target object is at least as high as that of the source object. This is intended to prevent the so-called "write-down" effect in which the classification level of information is gradually diluted as it is passed between data objects (e.g. files) of different

classifications.

Your Own Classification System

Now, all of this may seem just a little complex. That's because it is. Such a formal approach may not be necessary in all organizations; however, those in charge of developing security policies should develop a classification system as well as a supporting rule set that will support the requirements and objectives of the organization.

In the next few paragraphs I'll outline a simple system that can be applied to both information and *information technology* and is flexible enough to work in most types of organizations. Later, I will refer to this classification system when I give some example policies.

Ownership

Every piece of corporate data is assigned to an owner. By default, the owner is the creator of the data or the person who loaded the data onto the organizations systems. If it is not clear who the owner is, ownership then defaults to the originator or the administrator of the system on which the data resides. The owner of a computer system is defined as the head of division requesting the installation of equipment.

Classification

All data has a default classification (refer to the sections that follow) but with sufficient justification, the owner of the data may change the classification. Data may only be changed with sufficient justifiable reason. The user will ultimately be held responsible for data that has been reclassified. If the user is not sure about changing the security level, the Security Manager or divisional manager should be consulted. The person changing the security level will be held responsible for changing the level and must therefore be able to justify the decision.

Computers are classified in a similar way as data. Each computer has an owner defined as the head of the division requesting the installation of the equipment and it's the function of the equipment owner to classify all equipment under his or her control. Classification is done in consultation with the owner (or an assigned representative) and the Security Manager but the Security Manager must make the final decision. There may be a predefined list of classifications for computers in the network security policy. In addition to computers themselves, specific

services or processes can also be classified. For example, on a UNIX machine used to host web a public web site, the web server may be classified in one way whilst the telnet server has a much higher security level.

The Security Manager must also classify segments of the network and physical locations on the premises to ensure that computers are connected at the correct location on the network.

Clearance

Finally, all users and potential users should be classified. A user's classification is called a *Clearance Level* and is used to determine what data and resources a user may have access to. In general, access is only allowed when the clearance is the same level or higher than the classification of the item being accessed (data, equipment or physical locations).

Security Levels

Let's review the security levels. You must define and describes levels of classification that make sense and are appropriate to your organization. I've already listed the levels typically used in the military model. Another approach may be as follows:

- **Unclassified:** Considered publicly accessible. There are no requirements for access control or confidentiality.
- **Shared:** Resources that are shared within groups or with people outside of your organisation. This can include mail servers that are accessible from the Internet, servers that are accessible from customers and routers that link you to your ISP. Data that is legitimately accessed by outside people or groups can be classified as shared and users from outside organizations that have legitimate access to internal resources could also be classified as shared.
- **Company Only:** Access to be restricted to your internal employees only.
- **Confidential:** Access to be restricted to a specific list of people. For someone to have access to data or resources classified as 'Confidential' they must be cleared at this level and they must be included in the access list for this resource. The owner of the object (data or computer) is responsible for managing the access lists.

Not only data but also Users are *cleared* according to this system. Every user requiring access to your systems must receive clearance first. This includes employees, contractors, consultants etc.

An example Access Matrix

Once you've finalized a classification system a simple access matrix can then be drawn up:

Access Control Matrix				
USER	OBJECT (Data, Equipment, Physical Location)			
	Unclassified	Shared	Customer Only	Confidential
Unclassified	Allowed	Denied	Denied	Denied
Shared	Allowed	Allowed	Denied	Denied
Company Only	Allowed	Allowed	Allowed	Denied
Confidential	Allowed	Allowed	Allowed	Refer Access List

A matrix such as the one above can form a guide when writing a policy and the example policies given in this document do make use of this system.

Rules for technology

The matrix above deals with user access to objects. To describe where equipment is connected to the network, there is a very *simple rule*:

The Very Simple Rule:

1. Equipment may never be connected to a network segment with a different security level to that of the equipment.
2. Equipment may never stand in a physical location with a lower security level than that of the equipment.

Default Classifications

It was mentioned previously that objects could have default classifications. The idea behind default classifications is to minimize the workload on users and security staff whilst still ensuring that the proper security controls are always applied.

Here is an example of default classifications:

Default Classifications		
Object Type	Default Classification	To Change Classification
Data	Company Only	User discretion and responsibility
Equipment	Company Only	Request to Security Officer
Network Segment	Company Only	Request to Security Officer
Physical Location	Company Only	Request to Security Officer
User	Unclassified	Request to Security Officer

Of course, all of the above serve as examples only. Obviously, final decisions of classification must lie with the Security Officer and the Security Task Group described earlier in this paper.

Next time?

This concludes the second installment in our four-part series discussing security policies. In the next installment, we will be looking at structuring and implementing policies in a manner that will ensure that they are effective and practical.

References

[1] Snow, Dick; Department of Computing Science, University of Newcastle upon Tyne; "Security Models"

To read **Introduction to Security Policies, Part Three: Structuring Security Policies**, click [here](#).

Relevant Links

[Introduction to Security Policies, Part One: An Overview of Policies](#)

Charl van der Walt

[Privacy Statement](#)

Copyright 2006, SecurityFocus