



The SYSTEMS CONSULTING CONSORTIUM, Inc.
Research Report
Author: Larry Marks
Date: September 2004

Security Inside Out

How To Make A Security Policy Cover The Most Serious Threats

ISSUE

Most corporate security policies have been designed to protect against attacks from the outside, but in spite of that, many fail to keep information inside. That's because most successful security attacks are "inside jobs" – the work of employees or contractors who are inside the organization. This paper discusses how companies can assess their readiness and take action to protect against this threat from the inside.

BACKGROUND

Last Year, companies spent, on the average, around 85% of their security dollars on countering threats from outside the company. We hear regularly about malicious computer viruses, massive denial of service (DoS) attacks and spyware (and other forms of Trojan Horse attacks.) Companies are right to be concerned about the risks posed by these attacks from the outside, but is this lopsided emphasis on external threats really justified? Consider the following:

- Gartner Group estimates that over 70% of attacks that resulted in economic loss to companies involved a company insider.
- The same Gartner analyst estimates that as much as 95% of computer crime that results in significant loss to companies involved a company insider.
- The average economic loss resulting from insider attacks was about \$125,000 in 2003.
- A Michigan State study concludes that up to 70% of all identity theft crime begins with the theft of personal data by an employee.

These statistics suggest that many companies may need to re-examine their security policies with a focus on internal security threats.

HOW CAN COMPANIES ACT AGAINST INTERNAL THREATS?

Creating a security policy intended to counter threats from the inside is a tricky affair. Erecting too many barriers can reduce productivity and demoralize workers, but too little protection can leave the company and its customers open to damage from internal attacks.

The majority of expense to create such a security policy will be in the development and enforcement of the policy. Little new hardware, software or technical expertise is likely to be needed.

Below, in general terms are seven things to consider in developing and implementing the new security policy. Of course, a security audit including a thorough risk analysis, should be performed in order to

guide the process, while specifics of security services and mechanisms should be determined at the time the security policy is to be implemented.

1. Decide what to protect

A good security policy must specify both what to protect and how long to protect it. These criteria are very important. Protecting objects that intrinsically have no economic impact or objects that no longer have economic impact provides no benefit. Worse, it is a waste of money and resources, and may even impair security objectives:

- Employees will spend more time on tasks by having to deal with a security system
- More computer power will be required for the operation of the security mechanisms
- Attitudes about security will become lax, thus endangering objects of real value.

When deciding what to protect, the security policy should specify the criteria used to evaluate and balance several factors. The most common of these are:

- The potential economic damage to a company, client or customer resulting from hostile use of data or an illicit transaction
- The cost of protecting the object using various available mechanisms.
- The length of time that the object must be protected.

Some examples may serve to explain the relationship between these factors.

Example 1: Access to information about or transactions against a bank account. Such objects must be continuously protected. But how much should be spent on protection? Using historical data as a basis, banks will strike a balance between a tolerable loss and the cost of protecting the object.

Example 2: Quarterly results of a publicly traded corporation. Insiders develop and are aware of the quarterly results for some time before their release to the public. Early release of this information, either voluntarily or involuntarily, could lead to substantial economic loss to the corporation in the form of fines and unprepared market reactions. It is clearly worth protecting, but for how long? Once the information is published, there is no longer any value in protecting it, only cost.

2. Determine how the object will be stored

For some protected objects, it may be acceptable to permit many copies of the object to exist on various desktop or laptop computers. These objects may be further protected through encryption and watermarking. For example, a company pricelist is certainly of value to a competitor, but practicality may require that sales personnel have pricelists on their laptops. Encryption will protect against access to sensitive objects should the system be lost or stolen. A watermark will guarantee the authenticity of the object and can also be used to identify the source of a leak.

The most sensitive objects should be stored encrypted on as few systems as possible and access to the

systems, and to the objects on these systems, should be controlled. In extreme cases, systems may be isolated from all internal and external networks, providing access to objects only from carefully controlled physical locations. For example, a back-office worker will often require access to sensitive company or personal information. That information need not be distributed among a large number of systems; rather it need reside on at most a few servers. Access to the servers and the information can be carefully controlled.

3. Determine how a user's identity will be verified (authentication)

Access to objects in a secure environment is based on two factors: who you are (authentication) and what you are permitted to do (authorization).

Authentication is the service that determines whether or not a user is who s/he claims to be. In most cases, who you claim to be is a user id. There are three common mechanisms for verifying that you are who you claim to be:

- Something you know: This is typically a password or pass phrase. This is by far the most common authentication mechanism.
- Something you have: This could be a USB key or a Smart Card.
- Something you are: This is most typically a biometric measurement (voiceprint, finger print, etc.)

For many objects, authentication by a password provides sufficient protection. This is also called *weak authentication* because only one mechanism is used. For objects requiring a higher level of protection, a combination of mechanisms, or *strong authentication* can be used.

4. Determine how a user's authority will be verified (authorization)

Authorization is the service that determines the access that a properly authenticated user has to an object. Examples of the types of access that a user may or may not be authorized include:

- Create permission: The ability to create a new object
- Delete permission: The ability to erase an existing object
- Copy permission: The ability to make a copy of an object
- Modify permission: The ability to change an existing object
- Use/View permission: The ability to use or view an object
- Print permission: The ability to print an object that is printable

Each user need have only those permissions that are required by that user to do the job. Even senior executives should have only those permissions that are necessary to do the job.

5. Determine how authentication and authorization data will be administered

Authentication and authorization data are necessarily protected objects and are usually stored in an encrypted format. They are most frequently administered by the Human Resources organization. One reason that most companies cite for this arrangement is the fact that most personal data about

employees is already under the control of HR. Another reason frequently cited is that it creates a separation of control. The protected objects and the systems on which they reside are typically under the control of the IT department. Access to the systems and objects is under the control of the HR department. This makes it harder for an insider to breach security, since it would require a broader conspiracy to do so.

Most companies limit access to authentication and authorization data to a few highly trusted administrators. Many companies require simultaneous action by two or more administrators in order to make changes to authentication and authorization data.

6. Make an audit trail of all access to protected objects

All access mechanisms for protected objects must create an unmodifiable, protected audit trail, with an entry for each attempt, successful or not, to access a protected object. This is one of the most important and valuable mechanisms in the internal security toolbox. It is essential in order to enforce the internal security policy. Experienced auditors can regularly examine the audit trail to uncover patterns of abuse, and investigators can use it as evidence in cases of computer crime. Watermarks placed in the audit trail while it is being created can be used to determine if an audit trail has been tampered with.

7. Control the environment where sensitive data is used

No matter how many security mechanisms are in place, it will be difficult to protect objects if the environment where they are stored and used is not physically protected. Things to consider in establishing a secure environment include:

- Employee awareness of and executive leadership in adhering to the security policy
- If at all possible, use strong authentication or a single mechanism other than passwords
- Immediate revocation of authorizations in case of termination, lost hardware, etc.
- Physically secured storage facilities and, in some cases, access terminals
- Inspection of worker effects on entering and leaving the work area
- Absence or careful control of materials to which information could be copied

It is a challenge for any company to maintain an environment in which sensitive materials can be protected while not alienating employees. Of course, no company can function without a certain level of trust accorded to all employees, so a security policy may not provide total security. But a good security policy can protect against the most serious intrusions, while making employees feel comfortable that they won't be unjustly accused of a computer crime.

This report was prepared by the Systems Consulting Consortium, Inc. (SCC) as a service to our past, present, and future clients. SCC provides I/T Security services of the kind described herein. For more information about SCC, please visit our website at www.scc.cc or contact us directly at:



The SYSTEMS CONSULTING CONSORTIUM, Inc.
P.O. Box 519, Orinda, CA 94563-0519
925-254-0760, 925-254-8524 fx, www.scc.cc