Interested in learning more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Guidelines for an Information Sharing Policy

Information is often an organizations most valuable asset. As such, it is a high priority that information is secured with a high degree of confidentiality, integrity, and availability. One method of enhancing information security is through the creation of security policy. However, while policy works well at the global program level within an organization, how can it be used to fit the needs of individual the organizational units? The use of information amongst users and co-workers in these organizational units presen...

Copyright SANS Institute
Author Retains Full Rights

AD

Guidelines for an Information Sharing Policy

Chris Gilbert
GSEC - ver. 1.4b option 1

Abstract

Information is often an organizations most valuable asset. As such, it is a high priority that information is secured with a high degree of confidentiality, integrity, and availability. One method of enhancing information security is through the creation of security policy. However, while policy works well at the global program level within an organization, how can it be used to fit the needs of individual the organizational units? The use of information amongst users and co-workers in these organizational units presents interesting challenges for policy which must be addressed in a unique way.

This paper presents a set of guidelines which may be used in the creation of an Information Sharing Policy for small organizational units. To help facilitate these guidelines, a general overview of effective policy creation is presented. Following the step-by-step Information Sharing Policy guidelines, specific examples of the policy's use are set forth. Concluding remarks include information on increasing policy effectiveness and awareness.

Introduction

For many types of organizations in the public and private sector, information is the most valuable asset. Corporate marketing units may rely on their press contact information, university research departments may rely on their experimental data, and non-profit organizations may rely on publications they distribute. Information resources are utilized and relied on by many people throughout an organization. Unfortunately, since the most valuable asset is also the most widely used resource, a certain degree of security is required to guarantee the confidentiality, integrity, and availability of this information.

One method of information security is to write and enforce policy which dictates the procedures for using information. Policy is a scaleable security measure because it can exist at any level of an organization; from global corporate mandate down to workgroup issue-specific policy. The highest-level policy for organizations will often declare acceptable use of information systems, state that the organization is the owner of all information created or used on these systems, and grant themselves the right to audit, monitor, or inspect any of the systems. Additionally, organizations may limit employee privacy with language such as:

> "Users have no reasonable expectation of privacy concerning any materials transferred over or stored within the network."[1]

The enforcement of global, program policy such as this works well to set the general tone for information security throughout the entire organization.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

But how do these global policies scale to the level of the department, business unit, or workgroup? Different organizational units may have specialized needs that are not covered by the all-encompassing program policy. This paper will focus on a specific need of smaller business units which is often not addresses by program policy; the need for security in information sharing.

Background

Whether they are called strategic business units, departments, bureaus, or workgroups, the employees of organizational units often need to work together and share information to accomplish their specialized functions. The institute which I work for is part of a research university and has a common culture of teamwork to accomplish goals. More than one person may be entering data in a database, documents may have multiple authors, and network shared space is commonly used to move project files between project members. The trust in information sharing is so strong that if a person critical project member is absent from work, their computer may be accessed by co-workers to retrieve data as necessary. A lack of incidents has maintained a high enough level of trust for this information sharing to continue.

Unfortunately, the security of information is at risk by simply being stored and accessed on a networked computer. The risk of an incident is even more significant when multiple people will be legitimately modifying, updating, and otherwise accessing the data on these systems. Who is held accountable for the contents of a document with multiple authors? Who should access the files of a terminated employee? Who should be allowed to view a co-worker's files if they are needed in an emergency? Clearly, information sharing poses a threat to confidentiality, availability, and integrity.

During my time with the institute thus far, I have taken certain technological steps to improve security in the face of information sharing. To improve authentication and introduce the concept of file permissions, all desktop systems were upgraded from their various Windows 9X operating systems to the more secure Windows 2000. To grant users different levels of permissions, domain user groups were set up. To improve different users' data isolation and security on general access computers, multiple project-specific user accounts were created.

However, the information security measures must comply with the organization's policy. In my case, policy states that the institute owns all content created using its systems and that it may audit its systems at any time. In order to give the institute the power to audit, users' domain passwords were put on file in a secure location which could only be accessed by two staff members; myself included. Unfortunately, while this password file was a key to compliance with institute policy, it could be leveraged by employees to gain access to each other's files for legitimate or unauthorized purposes. This remaining lack of security presents the

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

clear need for an issue-specific departmental policy to handle the sharing of information.

Overview of Policy

Before an information sharing security policy can be written, the details of policy should be explained. The Merriam-Webster English Dictionary defines policy as, "a definite course or method of action selected from among alternatives and in light of given conditions to guide and determine present and future decisions."[2] Essentially, this defines policy as the chosen rules and procedures which will dictate future actions.

There are many essential steps to creating a document with the power to dictate future actions. In his preparation guide to information security policy, David Jarmon suggests that security policy has a cyclical life cycle consisting of risk review, policy creation, implementation, administration, and audit.[3]

The risks of information sharing have been introduced earlier in this paper; they present a threat to the confidentiality, integrity, and availability of information. The process of policy creation is a detailed process in which the "rules and procedures which will dictate future actions" will be chosen. Michele D. Guel suggests a policy design process involving choosing a policy design team, creating the policy, then reviewing the policy with management and the staff members who are effected by it.[4] Following this process will help achieve greater acceptance of policy by both management and staff. Additionally, having input and approval from organizational management throughout the policy creation stage will give them enough vested interest to make policy administration and enforcement possible. Finally, the process of policy audit will measure the policy's effectiveness and suggest areas of revision, thus returning the policy life cycle to the risk review and creation stages.

The guidelines for successful policy implementation may help create a security policy, but to create an effective security policy, there are a few other elements to consider. RFC 2196, the indispensable guideline for security policy creation, lists characteristics and components of a good security policy. They suggest that policy must be reasonably implementable, reasonably enforceable, and must clearly define responsibility.[5] Additionally, the language of the policy must be understandable, realistic, and must not restrict the freedoms of users to the point where productivity is diminished.
Ensuring that these elements are included in the security policy will help make it a more valuable resource. Having completed the overview of policy, the guidelines for an Information Sharing Policy can be described.

Identify Assets, Threats, and Countermeasures

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Overcoming the security issues associated with information sharing can be difficult, but a carefully created policy will ensure a higher degree of safety.

To begin, the information which needs to be protected must be identified. Before a department can define protected information, they should check the policy of their greater organization for definitions of protected information. Additionally, the organization's program policy may or may not grant departments the right to override certain aspects of the program policy.

Information which needs to be protected:

- Information created by, intended solely for, or of sole possession of a single user.
- Information considered personal or private to a single user.
- Information relating to employee health or social security number, Non-disclosure Agreement protected information, publicly identifiable research subject or customer data, classified information, and information protected by the greater organization's program policy.

It is important to protect information which is considered solely for a single user. Users may store work-related information which is not intended for release such as pending press releases, opinions or personal notes about vendors or other contacts, project journals or other forms of tracking progress. Also, non-work-related personal or private information may have a right to be protected. However, though one goal is to protect the confidentiality and privacy of information, access authorization may be granted to certain employees through departmental or organizational Ownership Policy or Audit Policy.
If organizational policy indicates that users have "no reasonable expectation of privacy", they must be made aware that their information is subject to monitoring or searching at the employer's discretion. Additionally, case law has shown that when the reasonable expectation of privacy is denied, a search of user information does not violate their 4th amendment right to privacy.[6]

To help determine which protective countermeasures will be employed, the threats to the protected information need to be determined.

Threats to information which must be reduced:

- Breach of user confidentiality or privacy due to unauthorized access of protected information.
- Breach of information integrity, ownership, or accountability due to unauthorized modification of protected information.
- Breach of information availability due to unauthorized deletion, movement, or other suppression of protected information.

Though these threats are posed by forces outside the organization, separate policy (such as policy for router configuration, firewall configuration, or anti-virus

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

protection) must help mitigate those threats. The focus of the information sharing policy is to mitigate the threat from other users within the organizational unit.

Having defined protected information and the things which threaten it, solutions for ensuring its protection may now be explored. With such a focus on "unauthorized access," it may be easy to overlook one large countermeasure; policy outlining legitimate access. Policy which outlines the legitimate access and storage of protected information will help to reduce the chance for incident from an identified threat.

Preventative measures to increase security from identified threats:

- Users must store any information intended to be protected in a password or otherwise authentication protected storage area.
- Users intending to share any information for viewing only must take appropriate technological steps to deny modification of that information.
- Users must not release their password or other methods of authentication (ie: keys, access cards, etc) to other users who are not specifically authorized to receive such access.
- Information to be shared with a group of users must be placed in a protected storage area which grants access only to the authorized users. This storage area will be created by the system or network administrator upon request. A standard request procedure must be created to ensure consistency. Upon completion of the use of the protected storage area, a request for deletion will be sent to and carried out by the system or network administrator.

Similarly to the assessment of information threats, many of these user-based threat deterrents rely on additional external documents such as password and authentication policy.

Returning to the primary focus on preventing unauthorized access, a common threat of unauthorized access is posed when users' information is legitimately needed by other users. If a project team needs access to files stored on a team member's computer in their absence, the process of accessing those documents poses a threat. If an employee who is central to the department's communication strategy is on vacation, the process of an assistant legitimately accessing their voicemail poses a threat. If an employee needs information managed by a previous employee of their position, accessing the terminated employee's information poses a threat.

To enable the legitimate access of other users' information, a solution was gleaned from a recently updated law in the state of New Jersey. New Jersey's "Public Access to Governmental Records Law" declares that government records (with certain exceptions) are accessible for inspection or examination by the public.[7] Not only does this give the public access to government records, but also to records of state funded organizations such as state universities.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Examination of the full text of the law shows that this incredible amount of access is handled by records custodians; defined as "the officer officially designated by formal action of that agency's director or governing body"[8] All requests for access to information must be forwarded to the custodian of records. The custodian then enforces the law by receiving the information and distributing it to the requestor in a timely fashion.

This model of information access could be implemented in policy at the level of the organizational unit. Since a function of policy is to assign responsibility, the job of the information custodian could be clearly defined.

Role and responsibilities of the information custodian:

- The information custodian is responsible for receiving, granting or denying, and fulfilling users' requests for protected information belonging to other users.
- The custodian is granted full authorization to access protected systems and other restricted access material in order to fulfill information requests.
- The custodian will create and maintain a collection of passwords and any other authentication materials necessary to carry out information requests. This compiled authentication resource must be protected with a high level of security which will be determined by the department's unique environment. Only the custodian may have access to and may utilize this resource.
- While the custodian may encounter protected or confidential information, the custodian agrees to not access, acquire, use, copy, or transfer this information except to the extent necessary to fulfill the information request.[9]
- In the event of the absence of the information custodian, non-urgent requests may be differed until the custodian's return or urgent requests may be handled by another custodian or user with higher authorization who agrees to the terms of non-disclosure.

The final definition of the information custodian's responsibility depends on the specific (and often unique) circumstances of the users within an organizational unit. The above guidelines serve as a baseline for the information custodian's responsibility. In order for the policy to remain flexible, there must be provisions for the case that an exception must be made. These provisions rely heavily on the culture of the unit to which the policy applies and, thus, are omitted here.

In order to better understand the role and responsibility of the information custodian, specific common examples of information sharing and access requests will now be explored.

Computer Login Access

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

A primary duty of an information custodian will be the routine access of the computers of individual users. Policy dictates that the custodian is the only other user with access to log in to a user's computer AS that user. This policy is enforceable through the use of logging. Local computer and authentication server logs will help hold the custodian accountable for his or her actions. As well, these logs will help to reveal any unauthorized access; if a login was recorded for a user who was not at work and the custodian was accounted for elsewhere, an incident of confidentiality breach has occurred. The consequences and actions of this breach will be dealt with by the Password Protection Policy, or a policy of equivalent content.

Document Access

It may be extrapolated from the policy that, in the event of an information request, the data custodian is the one to access the stored password file, authenticate as the target user, and find the requested files. I may speak from personal experience and say that, often, an information request may be rather vague, requiring the custodian to search within files to find the necessary information. It is the duty of the information custodian to ensure that the information to be relinquished meets the criteria of the request. If incorrect information is relinquished to the requesting party, a breach of confidentiality has occurred. The information custodian must take the necessary steps to act as an unbiased third party in order to refine the request from the requestor without releasing the incorrect information.

The custodian's job is made easier by the "user's preventative measure" section of the policy. It is the responsibility of the enforcing agent of the policy to ensure that users (specifically of multi-user systems) comply with storing their information in authentication protected storage spaces. A breach of confidentiality, integrity, or availability as a result of protected information being stored improperly is a fault of the owner of that data and repercussions will be applied appropriately.

E-mail and Voicemail Access

In the event that a custodian must access a user's e-mail or voicemail to gather requested information, the custodian is held to the highest level of confidentiality. Any information unrelated to the request which is overseen, either personal or work related, must be kept confidential. These terms of confidentiality apply to all aspects of the custodian's duties.

Terminated Employee Information Access

Managing the information of a terminated employee is a key part of the information custodian's position. Some organizations dictate that the terminated

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

employee retains privacy of his or her own information and need only relinquish it to the previous employer at his or her discretion. Though this right of privacy is generous to the employee, vast amounts of information may be lost upon sudden termination or because of an unwilling ex-employee. Thus, it is necessary to have a program policy which dictates organizational ownership of all information created by employees. This will give an information custodian access to retrieve the information of a terminated employee.

Though not suggested in the above guidelines, it may be a benefit to the privacy of the terminated employee if the custodian becomes temporary owner of their information. While possessing ownership of the information, the custodian should remove any personal or otherwise sensitive information that does not apply to the duties of the ex-employee. Once purges, the custodian may then relinquish the entire body of information to a new employee who fills the vacant position. If the vacant position is not filled, the custodian retains ownership and custody over the information and is required to keep them private and secure as outlined by policy.

Conclusion

An Information Sharing Policy may be met with much resistance in a small organizational unit, especially if there were no such measures previously in place. Like all security measures, policy will slow down progress and add another layer of complexity to the operations of the users. However, the increased security which is gained by an Information Sharing Policy is substantial and beneficial to the users it is governing. If users are hesitant to comply with the policy, present them with the scenario of a co-worker illegitimately accessing a copy of their resume. When it is seen that this sort of access will be protected by an Information Sharing Policy, it may be more widely embraced.

When (and if) such a policy is embraced by the management and users, it may quickly cease to be felt as a burden to progress. If users are aware of the extra steps necessary to request protected information, they may build that time into their schedules. Also, if users are aware that their data is not private, they will take steps necessary to ensure that no private information resides on the information systems.

Ultimately, an Information Sharing Policy is effected by the organizational unit's uniqueness. No two departments work alike and, thus, no two Information Security Policies will be alike. However, the confidentiality, integrity, and availability of information will always be further protected by the access rights defined by an Information Sharing Policy.

References

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

[1] "WRSD Information Network." URL: http://www.winnisquam.k12.nh.us/Technology/HSMSAUP.htm (1 Feb. 2003).

[2] "Merriam-Webster OnLine." URL: http://www.m-w.com/ (2 Feb. 2003).

[3] Jarmon, David. "A Preparation Guide to Information Security Policies." 12 March 2002. URL: http://www.sans.org/rr/policy/prep_guide.php (27 Jan. 2003).

[4] Guel, Michele D. "A Short Primer for Developing Security Policies." 2001. URL: http://www.sans.org/resources/policies/Policy_Primer.pdf (27 Jan. 2003).

[5] Fraser, B. (Editor), Various (Authors). "RFC 2196: Site Security Handbook." September 1997. URL: http://www.ietf.org/rfc/rfc2196.txt?Number=2196 (25 Jan. 2003).

[6] Samson, Martin H. "United States of America v. Eric Neil Angevine." URL: http://www.phillipsnizer.com/int-art259.htm (1 Feb. 2003).

[7] Wall, Barbara Wartelle. "New Jersey strengthens its public-records law (January 25, 2002)." 25 January 2002. URL: http://www.gannett.com/go/newswatch/2002/january/nw0125-4.htm (9 Feb 2003).

[8] Various (Authors). "P.L.2001, c.404 (A1309 5R)." 8 January 2002. URL: http://www.njleg.state.nj.us/2000/Bills/PL01/404_.htm (9 Feb. 2003).

[9] "Information Technology Services." 17 June 2002. URL: http://its.baylor.edu/policies/BU-Confidential-Info.htm (9 Feb. 2003).

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Last Updated: May 25th, 2013

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Malaysia @ MCMC 2013	Cyberjaya, MY	Jun 03, 2013 - Jun 08, 2013	Live Event
SANS Pen Test Berlin 2013	Berlin, DE	Jun 03, 2013 - Jun 08, 2013	Live Event
Industial Control Systems Security Training - Houston	Houston, TXUS	Jun 10, 2013 - Jun 15, 2013	Live Event
Security Impact of IPv6 Summit 2013	Washington, DCUS	Jun 14, 2013 - Jun 16, 2013	Live Event
SANSFIRE 2013	Washington, DCUS	Jun 14, 2013 - Jun 22, 2013	Live Event
SANS Canberra 2013	Canberra, AU	Jul 01, 2013 - Jul 13, 2013	Live Event
Digital Forensics & Incident Response Summit 2013	Austin, TXUS	Jul 09, 2013 - Jul 16, 2013	Live Event
SANS London Summer 2013	London, GB	Jul 09, 2013 - Jul 16, 2013	Live Event
SANS Rocky Mountain 2013	Denver, COUS	Jul 14, 2013 - Jul 20, 2013	Live Event
SANS Mumbai 2013	Mumbai, IN	Jul 22, 2013 - Jul 27, 2013	Live Event
SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification	Washington, DCUS	Jul 22, 2013 - Jul 26, 2013	Live Event
SANS San Francisco 2013	San Francisco, CAUS	Jul 29, 2013 - Aug 03, 2013	Live Event
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	Bangalore, IN	Aug 05, 2013 - Aug 10, 2013	Live Event
SANS Boston 2013	Boston, MAUS	Aug 05, 2013 - Aug 10, 2013	Live Event
Critical Security Controls Summit	Washington, DCUS	Aug 12, 2013 - Aug 18, 2013	Live Event
Industrial Control Systems Security Training - DC	Washington, DCUS	Aug 12, 2013 - Aug 16, 2013	Live Event
SANS Thailand 2013	Bangkok, TH	Aug 19, 2013 - Aug 31, 2013	Live Event
SANS Virginia Beach 2013	Virginia Beach, VAUS	Aug 19, 2013 - Aug 30, 2013	Live Event
Mobile Device Security Summit 2013	OnlineCAUS	May 30, 2013 - Jun 06, 2013	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced