Writing InfoSec Policies

Charles Cresson Wood, CISA, CISSP

Baseline Software Inc, PO Box 1219, Sausalito, California 94966, USA.

Introduction

No matter how sophisticated the information security technology, controls will not be sustainable unless the human element has been adequately addressed. Too many people look at information security as strictly a technological problem, when in reality it is both a technological and a human problem. For example, setting up a firewall alone does not guarantee that Internet access will then be secure. One must also address a host of related considerations such as policies, procedures, standards, and other management instructions. These might, for example, let workers know that representations on external networks must always be accompanied by words which clearly indicate they do not represent the organization's official position.

In the marketing field there is a useful concept called marketing-mix. This defines the combination of approaches for marketing a particular product or service. For example, telemarketing, mass mail, advertising, and trade shows might be used to generate leads for a new software product. The most effective balance of these approaches will be unique to each vendor. Similarly, in information security there is a proper controls-mix that is unique to each organization. This controls-mix is made up of both technological and human factors. For a bank it might, for instance, include encryption, digital signatures, special transaction audit trails, among other technological factors, as well as user training classes, computer-based training courses run off of personal computers, as well as a written manual containing information security policies.

To come to the proper controls-mix for a particular organization, one must first perform a risk analysis (also known as a risk assessment). There are many popular techniques for performing a risk analysis, including standard-of-due-care comparisons, quantitative risk analysis, scenario analysis, and penetration attacks. Whatever the technique employed, a risk analysis provides a unique perspective about the risks and controls found at a particular organization. It is only with this as background that one should embark on the an information security policy writing task. In other words, one must understand the special needs of an organization before one attempts to generate specific written management directives.

The balance of this paper is devoted to a clarification of the different types of written instructions that management can issue regarding information security, and some of the initial steps that one can take when embarking on the non-trivial task of writing information security policies. The material provided below has been extracted from the introductory section of the author's book/floppy-disk entitled *Information Security Policies Made Easy*.

What Are Information Security Policies?

Distinct from Guidelines and Standards

'Policies' are management instructions indicating how an organization is to be run. They are high-level statements intended to provide guidance to those who must

0167-4048/95/$9.50 © 1995, Elsevier Science Ltd

make present and future decisions. Some people prefer to think of policies as generalized requirements. Although they vary considerably from organization to organization, information security policies typically include general statements of goals, objectives, beliefs, ethics, and responsibilities, often accompanied by the general means for obtaining these things (such as procedures).

Policies are mandatory; special approval is required when a worker wishes to take a different course of action. They are distinct from, but similar to 'guidelines', which are optional and recommended. In fact, many policies can be easily transformed into guidelines simply by replacing the word 'must' with the word 'should'.

Policies are higher-level statements than 'standards', although both types of management instructions require compliance. Policies provide general statements, whereas standards make specific mention of technologies, methodologies, implementation procedures, and other detailed factors. Generally speaking, policies are intended to last for many years, while standards are intended to last for only a few years.

Standards will need to be changed considerably more often than policies because the personnel procedures, organizational structure, business processes, and information systems technologies mentioned in standards change so rapidly. For example, a network security standard might specify that all new or substantially modified systems must be in compliance with International Standards Organization (ISO) standard X.509 (which involves authentication of a secure communications channel via public key cryptography). This standard is likely to be revised, expanded, or replaced in the next few years.

Distinct from Procedures and Controls

Policies are distinct from and considerably higher-level than 'procedures' (sometimes called 'standard operating procedures'). Procedures are specific operational steps that workers must take to achieve a certain goal. For instance, in many data processing shops there are specific procedures for performing back-ups of mainframe disk packs. A policy statement describes only the general means for addressing a specific problem; it should not become detailed or lengthy — otherwise it becomes a procedure.

Policies are also different from 'controls' (also known as 'countermeasures', 'security measures', and 'safeguards'). An example of a control would be encryption of sensitive data stored on floppy disks. In many cases, policies provide broad objectives which are met with controls. For instance, a policy prohibiting actual or apparent conflicts of interest could be met via a control which requires that all employees sign a statement indicating they have read the code of conduct and agree to comply. On the other hand, some control measures are dictated directly by policy. For instance, the requirement to sign statements of compliance with a code of conduct might itself be a policy.

In general, policies state the areas on which management attention should focus. For example, a policy might dictate that all production software be fully tested prior to being used for production processing. Management in most instances will need to make a number of decisions about controls in order to meet the requirements of a policy. For example, the control measures in support of this testing policy could include production-program library management software, a standard development process methodology, documentation standards, and a set of standard testing procedures.

Why Are Policies Important?

Assuring the Proper Implementation of Controls

With hopes of handling information security expediently, management in many organizations simply purchases an information security product. In these cases, management often thinks the new product — be it hardware or software — is all that's needed. After the product is installed, however, management is all too frequently disappointed to learn that the hoped-for results have not materialized. This is often because the organizational infrastructure for such a product has not yet been established.

To establish a supporting organizational infrastructure, every organization needs documented policies, guidelines, standards, procedures, organizational responsibility statements, security measure enforcement procedures, a management oversight committee, a risk assessment process, and a security planning process. Policies and an initial risk assessment are the starting points for establishing an appropriate organizational infrastructure, i.e., they are the essence from which other elements of an infrastructure are derived.

Password-based computer access control packages provide a specific example. If management attempts to implement such a package without first having policies defining who should access what data, applications, systems, and networks, then confusion and emotional trauma are bound to result. Before an access control package is installed, management should first define policies like who has a recognized 'need-to-know', how such access will be granted, how such access will be audited, and other instructions. Likewise, if management attempts to implement such a package without knowing what information is at risk (as would be illuminated via an initial risk assessment), then trouble will be encountered.

Guiding the Product Selection and Development Process

Most organizations do not have the resources to design and implement controls from scratch. They often pick and choose among the controls provided by information security product vendors, and then they attempt to customize these controls with procedures, standards, and other organization-specific integration efforts. This custom integration process is often performed without sufficient understanding of the security objectives and goals of the organization. As a result, the security products chosen and their implementation may not be responsive to the true needs of the organization.

For example, a firm may have bought a call-back system thinking that this was the best way to secure its dial-up lines. Only later might it discover that many of its employees are using portable computers and that these employees need to dial-up the organization's systems from a variety of different locations including hotel rooms, client premises, and cars equipped with cellular modems. Call-back systems can be used only with great difficulty in those circumstances where users are calling-in from a variety of different locations. In this case, the purchase of dynamic password generators (also called an identity tokens) would have been preferable to the purchase of a call-back system.

Policies can provide both the understanding and additional guidance that workers need in order to act as management intends they should. Policies can accordingly be a way to make sure that in-house personnel are appropriately selecting, developing, and implementing systems.

Demonstrating Management Support

Some people (particularly users and data processing department staff) often say, "When management tells me to, I'll do something about information security." This attitude is not surprising when one appreciates that most people are unaware of the extent of the information security risks they face, just as they are not inclined to take the time to seriously analyze these risks. Beyond this, because they do not have the expertise, most people are unable to evaluate the need for certain control measures.

Policies are a clear and definitive way for management to demonstrate that (a) information security is important, and (b) workers should pay attention to information security. Policies can thus make up for circumstances that may otherwise cause people to insufficiently protect information resources. One frequently encountered example of this is middle level managers who keep refusing to include information security moneys in their budget. If policies dictating management support have been issued by top management, then middle level managers will not be able to continue to ignore information security.

According to a 1991 report issued by the National Research Council entitled *Computers at Risk*, a California prosecutor recently observed that: "We probably turn down more cases [involving computer break-ins] than we charge, because computer system proprietors haven't made clear what is allowed and what isn't." Don Ingram, a well-known district attorney in Alameda County, California, and an expert on computer crime, puts it concisely when he notes that "If you can't define it [inappropriate behaviour involving computers], how are you going to prosecute it?" Every organization should clarify the circumstances under which its computers are operated, so that when the time comes for prosecution or litigation, it will not be subject to these problems. Policies are a relatively inexpensive and straightforward way for management to define appropriate behaviour, demonstrate its concern, and specify which behaviours are acceptable/unacceptable.

In the above-mentioned National Research Council report, a board of information security experts indicated that: "A major conclusion of this report is that the lack of a clear articulation of security policy for general computing is a major impediment to improved security in computer systems" (page 51). The reader can address this major problem directly by developing policies uniquely responsive to the conditions found at his or her organization.

Avoiding liability

An increasingly compelling body of United States case law is demonstrating that people, particularly members of a management team, may be held liable for inadequately addressing information security matters. The basis for this liability can be: negligence, breach of fiduciary duty, failing to use the security measures found in other organizations in the same business, failing to exercise the due care expected from a computer professional (computer malpractice), or failure to act after an 'actual notice' (such as a compromise of security) has taken place. Discussions about liability exposure and the need for policies are often successfully used to gain additional management attention and support for information security efforts.

- Garner larger budget and more personnel.
- Establish top management communication path.
- Show definitive progress with minor investment.
- Establish info-security effort credibility and visibility.
- Shift attitudes and change perspectives.
- Demonstrate top management support.
- Coordinate activities of various groups.
- Achieve economies of scale.
- Avoid "cart before the horse" problems.
- Avoid "reinventing the wheel" problems.
- Guide security product selection and implementation.
- Assure consistent implementation of controls.
- Arrange contractual obligations needed for prosecution.
- Establish basis for disciplinary actions.
- Avoid liability for negligence, breach of fiduciary duty.
- Demonstrate quality control processes (ISO 9000 compliance).

Figure 1. Reasons to Establish Policies

The preparation and promulgation of relevant policies is an important way for management to demonstrate that it is concerned about and taking steps to address information security. To avoid liability, often it is enough to start work on information security and to set the direction for information security efforts. As attorney George S. Cole of Hagelshaw & Cole in San Francisco put it, "The first line of defence is that you are doing something about [information] security, not necessarily that you have it solved. Ignoring the thing, hoping it will go away, will crucify you."

Achieving Consistent and Complete Security

One of the significant problems in the information security field involves fragmented and inconsistent efforts. Too often one department will be supportive of information security efforts, while another department within the same organization will be resistant. To the extent that these departments share resources — such as a local area network — the resistant department will jeopardize information security in the supportive department. Although it is neither feasible nor desirable to make all persons in an organization familiar with the complexities of information security, it is important that they all subscribe to some minimum level of protection. In high-level terms, policies can be used to define this minimum protection level (sometimes called a 'baseline').

How Should Policies Be Developed?

Gathering Key Reference Materials

When developing a set of information security policies, the reader should reference a risk assessment that clearly indicates the organization's current information security needs. A loss history may also be helpful in terms of identifying areas in need of further attention. In order to identify the policy areas needing further attention, the reader should additionally have copies of all other relevant policies that are now in effect. These relevant policies include application system development policies, computer equipment acquisition policies, human resource policies, codes of conduct, and physical security policies. If they are readily obtainable, policies from other organizations in the same industry provide useful background information. If the reader's organization is a subsidiary or affiliate of another organization, then the other organization's policies should also be obtained and used as reference material.

Defining a Framework for Policies

After these reference materials have been compiled, the reader should then prepare a list of all topics to be covered in a new and more comprehensive set of information security policies. The list should include policies that are intended for immediate adoption as well as those intended for adoption some time in the future. This list should be prepared on a computer because it is likely to be revised several times.

The reader should then attempt to define the ways in which the organization expresses and uses policies. For example, policies may be expressed with the word 'must', and they may be placed in a standard operating procedures manual. Likewise, the organization may use policies to guide decision making and auditing efforts. The reader should also study the style in which existing policies are written, the use of certain words such as 'shall', the system for numbering and naming policies, as well as the linkages between policies and other management directives like procedures and standards.

Part of the reader's study of the existing policies and how they are used should entail a review of the level of detail appropriate for the organization's policy statements. The organization may have defined policies in quite specific terms, in which case many detailed policies may be appropriate. Alternatively, the organization may have defined policies in very high-level terms, in which case only a brief overall statement may be appropriate.

Information about the expression and use of policies is rarely written down, but it can be obtained by 'reading between the lines' of the existing policy statements, such as those issued by the Human Resources Department. To help ensure their prompt adoption, new information security policies should be written in a manner that resembles and can be used like existing policies.

Preparing a Coverage Matrix

After preparing a list of the areas needing attention, and after becoming acquainted with the ways in which the organization uses policies, the reader is now ready to create a matrix providing an overview of the topics that will be covered. A collection of policies can be used to generate ideas about the areas to be covered. Alternatively, the reader can compile their own collection from various sources including bits and pieces of material available over the Internet. A new list of needed policy categories (this can also be called a table of contents) should then be prepared with the information obtained thus far. This new list should be an augmented version of the same list of needs that was prepared earlier.

Most often policies will be directed at several significantly different audiences. In these instances, it is often advisable to have different documents tailored to the needs of the different audiences. For example, end-users might receive a small booklet with the most important information security policies that they need to keep in mind, while systems developers and other technical people would receive a considerably longer document that provides much more detail.

When several different audiences are to be addressed, the author recommends that the reader prepare a 'coverage matrix' before actually writing new policies. A coverage matrix is simply a tool to make sure that all the appropriate information security policy messages are presented to the appropriate audiences. It is a higher-level way of looking at the work to be done and as such can bring order to what otherwise may be a complicated policy writing effort.

A coverage matrix can be a simple two-dimensional table. It can, for instance, use the primary audiences to which the policies are directed (for example, end-users, management, Information Systems Department staff, customers, and business partners) as row identifiers, and required policy categories as column headings. The cells in the centre of the matrix could be filled with numbers separated by commas, each referring to a policy number. Figure 2 provides an example of a coverage matrix; note that the policy numbers appearing in this particular matrix are place holders and are not the result of an analysis as should be performed for each organization.

Control Categories Audience	Computers	Data Communication	Management	Physical
End-users	12, 35, 45, 46	12, 35, 46, 47, 48, 49, 56, 58	435, 436, 504	12, 35, 36
Management	12, 36, 37, 345, 401	304, 305, 307, 308, 309, 310	45, 47, 48, 49, 54, 55, 57, 59	35, 36, 37, 38, 44, 45, 134, 138, 213, 214, 216
Info Sys Dept.	34, 36, 59	189, 199, 200	501, 504, 523	12, 13, 14, 18, 222, 223, 224, 225, 226, 228, 229, 332, 336
Customers	234, 235, 236	202, 203, 204	34, 36, 38, 39	34, 35, 36, 38
Business Partners	256, 257, 258	205, 206, 207	40, 41, 42, 43	34, 35, 36, 39

Figure 2. Coverage Matrix Example

Because there will probably be many columns, but only a few rows, the author suggests that the reader prepare a standard coverage matrix with the rows filled in (for audiences), with blank column headings (for policy categories), and with blank cells in the middle (for specific policies). This template coverage matrix can then be copied many times to save the reader considerable time drawing coverage matrices. Alternatively, a spreadsheet program can be used with a standard coverage matrix.

The preparation of a coverage matrix presupposes that there should be separate policies for different groups within the organization. For example, the developers of business application systems are likely to need significantly more detailed security policies than end-users. Accordingly, a different set of policies, with some overlap, would be appropriate. If there is only one group of intended readers for the information security policies, the coverage matrix can be dispensed with. Often policy writers will at first anticipate that there is only one audience in need of policies, but after they become more acquainted with the project they then acknowledge that there are indeed several audiences.

The policies that are needed can now each be assigned a number, and each of these numbers may be entered into the coverage matrix. This procedure is very useful because it highlights the fact that certain groups to whom policies are directed are not being adequately addressed, just as it indicates that certain areas need additional policies to be truly responsive to the organization's needs.

The reader is urged to save the coverage matrix, because this same process may be useful in a year or two when the needs of the organization are appreciated in a more comprehensive way. The coverage matrix may also serve as important information in a court case, should there ever be any allegations that management did not seriously think about the risks and the policies that needed to be prepared. Similarly, internal and external auditors may wish to review the working papers which were used to derive the policies actually prepared.

When Should Policies Be Developed?

Before one embarks on an effort to write and obtain management approval for information security policies, it is advisable to clarify who is responsible for issuing and enforcing policies. Only when a clear assignment of responsibility for information security policies exists, should a policy development effort be initiated. This means that a centralized information security group mission statement and related job descriptions should be prepared and approved before a policy-writing effort gets underway. If these responsibility matters have not yet been clarified, this can be the first phase to a policy development effort. If this important step is ignored, be prepared for both interpersonal challenges and political objections which are likely to significantly delay progress.

Another necessary prerequisite for successfully writing information security policies, involves management's perspective. Only after management appreciates that information has become a critical factor of production, will information security be recognized as a matter deserving their attention. This perspective is known by a number of phrases including 'information resource management' and 'recognizing

information as an asset'. Management first needs to realize that they are responsible for managing information itself; then they will appreciate that new tools and techniques are needed. This is an appropriate time to mention the significant contribution that policies can make. If management doesn't really understand how important information is to their organization, they will be unlikely to support information security policy writing efforts.

Ideally, a policies development effort should be initiated after the performance of a comprehensive information security risk assessment. The risk assessment should indicate — perhaps only in high-level terms — the value of the information in question, the risks to which this information is subjected, and the control vulnerabilities found in the current way of handling this information. A risk assessment will provide useful background information with which the reader may determine whether the security policies are applicable and whether they will be cost effective. The general threat types faced by the organization, as well as other general background information from a risk assessment, may also be included in a written policy statement.

One of the best times to develop a set of information security policies is when an information security manual is being prepared. Because a manual is distributed widely throughout an organization, it is an excellent place to state information security policy. Specific written policies may also be prepared when compiling material for training and awareness efforts. These efforts may include a videotape, lectures, posters, or articles in an in-house newspaper. Another good time to prepare policies is right after a major information security breach, an unfavourable computer-related audit report, a security-related lawsuit, or some other type of loss which has received extensive top management attention. This is a good time to move ahead with policy development efforts because management — at these times — are especially supportive of and concerned about information security. At these times the practitioner should work fast because management's level of concern decreases very rapidly.

To provide direction for the preparation of system development guidelines, access control package implementation memos, computer technical standards, internal control procedural descriptions, and other more specific information security documents, policies should be prepared early in the life cycle of an information security effort. An initial set of policies is typically brief, and is followed by more detailed policy statements. A good objective to keep in mind when writing policies is that they should be written so that they need not be modified for five years.

To keep up with developments in organizational design, organizational mission statements, information handling technology, industry standards, laws, regulations, and other matters, it is important that information security policies be modified periodically.

Balancing Trade-offs

After having done research about information security policies, it should not be surprising if the reader finds a few policies which contradict other policies. For example, freedom of information policies often conflict with right to privacy policies. Each organization will need to determine where this and other lines should be drawn. Workers should be informed of these management decisions lest they be left to make these tough decisions on their own — often with catastrophic results.

Like many activities in the information security field, writing policies involves trade-offs. Frequently encountered trade-offs include those between cost and security, flexibility and security, as well as ease-of-use and security. There are many conditions and limits in the information security field, and policies must be designed to take these into consideration. For example, a policy dealing with the termination of employees for violating certain information security requirements may be incompatible with existing labour union agreements. For an information policy writing effort to be successful, the person who is writing the policies must understand the conditions and limits found in a particular organization. Such an appreciation for conditions and limits can be obtained by consulting internal audit reports, risk assessment documents, historical loss history analyses, and existing policies addressing other areas (like Human Resources).

Conclusion

Writing information security policies is an absolutely essential component of every successful information security effort. Policies set the stage for a wide variety of information security efforts such as assigning system privileges to users based on the need-to-know. Policies are also the primary way for management to communicate its intentions about the security of both systems and about the security of information itself. Even if your organization already has an information security policy statement, it is wise to review it every year to make sure it is still relevant and sufficiently covers the risks faced by the organization in question.

Charles Cresson Wood is an independent information security consultant based in the San Francisco Bay Area. In the information security field since 1978, his recent work involves specifying network security architectures, performing risk assessments, writing policies and standards, developing secure software, and developing new information security products. In addition to being the author or co-author of three computer security software packages, he is the author of three books and over 135 technical articles. His most recent book is entitled *Information Security Policies Made Easy*. He can be reached over the Internet at 3143490@mcimail.com.