CSO
FROM IDG

Credit: Thinkstock

How to write an information security policy

Learn the critical first step, why consensus is key, what to cover and how make your information security policy — and program — effective

By Jennifer Bayuk | JUN 16, 2009

An information security policy is the cornerstone of an information security program. It should reflect the organization's objectives for security and the agreed upon management strategy for securing information.

In order to be useful in providing authority to execute the remainder of the information security program, it must also be formally agreed upon by executive management. This means that, in order to compose an information security policy document, an organization has to have well-defined objectives for security and an agreed-upon management strategy for securing information. If there is debate over the content of the policy, then the debate will continue throughout subsequent attempts to enforce it, with the consequence that the information security program itself will be dysfunctional.

What to do first

There is a plethora of *security-policy-in-a-box* products on the market, but few of them will be formally agreed upon by executive management without being explained in detail by a security professional. This is not likely to happen due to time constraints inherent in executive management.

Even if it was possible to immediately have management endorse an off-the-shelf policy, it is not the right approach to attempt to teach management how to think about security. Rather, the first step in composing a security policy is to find out how management views security. As a security policy is, by definition, a set of management mandates with respect to information security, these mandates provide the marching orders for the security professional. If the security professional instead provides mandates to executive management to sign off on, management requirements are likely to be overlooked.

"If there is debate over the content of the policy, then the debate will continue throughout subsequent attempts to enforce it, with the consequence that the information security program itself will be dysfunctional."

A security professional whose job it is to compose security policy must therefore assume the role of sponge and scribe for executive management. A sponge is a good listener who is able to easily absorb the content of each person's conversation regardless of the group's diversity with respect to communication skills and culture. A scribe documents that content faithfully without embellishment or annotation. A good sponge and scribe will be able to capture common themes from management interviews and prepare a positive statement about how the organization as a whole wants its information protected. The time and effort spent to gain executive consensus on policy will pay off in the authority it lends to the policy enforcement process.

Good interview questions that solicit management's opinions on information security are:

- How would you describe the different types of information you work with?
- Which types of information do you rely on to make decisions?
- Are there any information types that are more of a concern to keep private than others?

From these questions, an information classification system can be developed (e.g., customer info, financial info, marketing info, etc.), and appropriate handling procedures for each can be

described at the business process level. *(Editor's note: See* Jason Stradley's provocative take on data classification and related issues*.)*

Of course, a seasoned security professional will also have advice on how to mold the management opinions with respect to security into a comprehensive organizational strategy. Once it is clear that the security professional completely understands management's opinions, it should be possible to introduce a security framework that is consistent with it. The framework will be the foundation of the organization's Information Security Program, and thus will service as a guide for creating an outline of the information security policy.

Creating a framework

Often, a security industry standards document is used as the baseline framework. For example, the Security Forum's *Standard of Good Practice* (www.securityforum.org), the International Standards Organization's *Security Management* series (27001, 27002, 27005, www.iso.org), and the Information Systems Audit and Control Association's *Control Objectives for Information Technology* (CoBIT, www.isaca.org). This is a reasonable approach, as it helps to ensure that the policy will be accepted as adequate not only by company management, but also by external auditors and others who may have a stake in the organization's Information Security Program.

> *"... where people are aware that there are no exceptions to policy, they will generally be more willing to assist in getting it right up front"*

However, these documents are inherently generic and do not state specific management objectives for security. So they must be combined with management input to produce the policy outline. Moreover, it is not reasonable to expect the management of an organization to change the way the organization is managed in order to comply with a standards document. Rather, the information security professional may learn about good security management practices from these documents, and see if it is possible to incorporate them into the current structure of the target organization.

Make it about mandates

It is important that security policy always reflect actual practice. Otherwise, the moment the policy is published, the organization is not compliant. It is better to keep policy as a very small set of mandates to which everyone agrees and can comply than to have a very far-reaching policy that few in the organization observe. The information security program can then function to enforce policy compliance while the controversial issues are simultaneously addressed.

Another reason that it is better to keep policy as a very small set of mandates to which everyone agrees is that, where people are aware that there are no exceptions to policy, they will generally be more willing to assist in getting it right up front to ensure that they will be able to comply going forward. Once a phrase such as "*exceptions to this policy may be made by contacting the*

executive in charge of...." slips into the policy itself or the program in which it is used, the document becomes completely meaningless. It no longer represents management commitment to an information security program, but instead communicates suspicion that the policy will not be workable.

A security professional should consider that if such language were to make its way into a human resources or accounting policy, people could thus be excused from sexual harassment or expense report fraud. A security professional should strive to ensure that information security policy is observed at the same level as other policies enforced within the organization. Policy language should be crafted in such a way that guarantees complete consensus among executive management.

> "The time and effort spent to gain executive consensus on policy will pay off in the authority it lends to the policy enforcement process."

For example, suppose there is debate about whether users should have access to removable media such as USB storage devices. A security professional may believe that such access should never be required while a technology executive may believe that technology operations departments responsible for data manipulation must have the ability to move data around on any type of media. At the policy level, the consensus-driven approach would produce a general statement that "all access to removable media devices is approved via a process supported by an accountable executive." The details of the approval processes used by the technology executive can be further negotiated as discussions continue. The general policy statement still prohibits anyone without an accountable executive supporting an approval process from using removable media devices.

Employing sub-policies

In very large organizations, details on policy compliance alternatives may differ considerably. In these cases, it may be appropriate to segregate policies by intended audience. The organization-wide policy then becomes a global policy, including only the least common denominator of security mandates. Different sub-organizations may then publish their own policies. Such distributed policies are most effective where the audience of sub-policy documents is a well-defined subset of the organization. In this case, the same high level of management commitment need not be sought in order to update these documents.

For example, information technology operations policy should require only information technology department head approval as long as it is consistent with the global security policy, and only increases the management commitment to consistent security strategy overall. It would presumably include such directives as "*only authorized administrators should be provided access capable of implementing operating system configuration changes*" and "*passwords for generic IDs should be accessed only in the context of authorized change control processes*." Another type of sub-policy may involve people in different departments engaged in

some unusual activity that is nevertheless subject to similar security controls, such as outsourcing information processing, or encrypting email communications.

On the other hand, subject-specific policies that apply to all users should not be cause to draft new policies, but should be added as sections in the global policy. Multiple policies containing organization-wide mandates should be discouraged because multiple policy sources make it more difficult to accomplish a consistent level of security awareness for the any given individual user. It is hard enough to establish policy-awareness programs that reach all in the intended community, without having to clarify why multiple policy documents were created when one would do. For example, new organization-wide restrictions on internet access need not be cause to create a new "internet access" policy. Rather, an "internet access" section can be added to the global security policy.

Another caveat for the security professional using the sub-policy approach is to make sure sub-policies do not repeat what is in the global policy, and at the same time are consistent with it. Repetition must be prohibited as it would allow policy documents to get out of sync as they individually evolve. Rather, the sub-documents should refer back to the global document and the two documents should be linked in a manner convenient for the reader.

Supplementary documents

Even while giving sub-policies due respect, wherever there is an information security directive that can be interpreted in multiple ways without jeopardizing the organization's commitment to information security goals, a security professional should hesitate to include it in any policy. Policy should be reserved for mandates. Alternative implementation strategies can be stated as a responsibility, standard, process, procedure, or guideline. This allows for innovation and flexibility at the department level while still maintaining firm security objectives at the policy level.

This does not mean that the associated information protection goals should be removed from the information security program. It just means that not all security strategy can be documented at the policy level of executive mandate. As the information security program matures, the policy can be updated, but policy updates should not be necessary to gain incremental improvements in security. Additional consensus may be continuously improved using other types of Information Security Program documents.

Supplementary documents to consider are:

Roles and responsibilities — Descriptions of security responsibilities executed by departments other than the security group. For example, technology development departments may be tasked with testing for security vulnerabilities prior to deploying code and human resources departments may be tasked with keeping accurate lists of current employees and contractors.

Technology standards — Descriptions of technical configuration parameters and associated values that have been determined to ensure that management can control access to electronic information assets.

Process - Workflows demonstrating how security functions performed by different departments combine to ensure secure information-handling.

Procedures — Step by step instructions for untrained staff to perform routine security tasks in ways that ensure that the associated preventive, detective, and/or response mechanisms work as planned.

Guidelines — Advice on the easiest way to comply with security policy, usually written for non-technical users who have multiple options for secure information-handling processes.

What an information security policy includes

This leaves the question: what is the minimum information required to be included in an information security policy? It must be at least enough to communicate management aims and direction with respect to security. It should include:

1. **Scope** — should address all information, systems, facilities, programs, data, networks and all users of technology in the organization, without exception
2. **Information classification** — should provide content-specific definitions rather than generic "confidential" or "restricted"
3. **Management goals** — goals for secure handling of information in each classification category (e.g., legal, regulatory, and contractual obligations for security) may be combined and phrased as generic objectives such as "customer privacy entails no authorized cleartext access to customer data for anyone but customer representatives and only for purposes of communicating with customer," "information integrity entails no write access outside accountable job functions," and "prevent loss of assets"
4. **Context** — Placement of the policy in the context of other management directives and supplementary documents (e.g., is agreed by all at executive level, all other information handling documents must be consistent with it)
5. **Supporting documents** — include references to supporting documents (e.g., roles and responsibilities, process, technology standards, procedures, guidelines)
6. **Specific instructions** — include instruction on well-established organization-wide security mandates (e.g., all access to any computer system requires identity verification and authentication, no sharing of individual authentication mechanisms)
7. **Responsibilities** — outline specific designation of well-established responsibilities (e.g., the technology department is the sole provider of telecommunications lines)
8. **Consequences** — include consequences for non-compliance (e.g., up to and including dismissal or termination of contract)

This list of items will suffice for information security policy completeness with respect to current industry best practice as long as accountability for prescribing specific security measures is established within the "supplementary documents" and "responsibilities" section. While items 6 and 7 may contain a large variety of other agreed-upon details with respect to security measures, it is ok to keep them to a minimum to maintain policy readability and rely on sub-policies or supporting documents to include the requirements. Again, it is more important to have complete compliance at the policy level than to have the policy include a lot of detail.

Note that the policy production process itself is something that necessarily exists outside of the policy document. Documentation with respect to policy approvals, updates and version control should also be carefully preserved and available in the event that the policy production process is audited.

Jennifer Bayuk is an information security consultant and former CISO. She has written or co-edited several books including Enterprise Information Security and Privacy, Stepping Through the IS Audit, 2nd Edition, Stepping Through the InfoSec Program, and a forthcoming work on Security Leadership.

"How to write an information security policy" originally appeared on CSO Online.