CHAPTER 46

DEVELOPING SECURITY POLICIES

M. E. Kabay

46.1 INTRODUCTION. This chapter reviews methods for developing security policies. Some of the other chapters of this *Handbook* that bear on policy content, development, and implementation are as follows:

- Chapter 15 provides an extensive overview of physical security policies.
- Chapter 18 discusses local area network security issues and policies.
- Chapter 25 reviews software development policies and quality assurance policies.
- Chapter 28 presents principles, topics, and resources for creating effective security policy guidelines.
- Chapter 29 looks at methods for enhancing security awareness.
- Chapter 31 provides guidance on employment policies from a security standpoint.
- Chapter 32 makes explicit recommendations about operations management policies.
- Chapter 33 reviews specific recommendations for e-mail and Internet usage.
- Chapter 35 presents concepts and techniques from social psychology to make security policy implementation more effective.
- Chapter 39 discusses the policies that apply to application design.
- Chapter 51 looks at censorship and content filtering on the Internet.

46.2 COLLABORATING IN BUILDING SECURITY POLICIES. Policies are the foundation of effective information security, but the task of policy creation is complicated by human and organizational resistance. Technology alone does not work. In changing human behavior, rationality and substance are not enough: The *process* of development affects how people feel about policies and whether they see these rules as needless imposition of power or an expression of their own values.

Security is always described as being everyone's business; however, in practice, security *interferes* with everyone's business. For example, network managers work hard to make networks user-friendly. They do everything they can to make life easier for users; they provide network access routines with a graphical user interface, client-server systems with hot links between local spreadsheets and corporate databases, and a gateway to the Internet for the engineering users. Superficially, one might think that implementing network security would

simply involve defining access controls, applying encryption, and providing people with hand-held password generators. Unfortunately, as discussed in Chapter 35, security policies offend deep-seated self-conceptions. People form close-knit work groups in which people trust each other; they do not lock their desks when they leave them for a few minutes, so why should they obey the network security policy that dictates locking their sessions? They even lend people car keys in an emergency; why should it be such a terrible breach of security to lend access codes and passwords to trusted colleagues in an emergency?

Security policies challenge users to change the way they think about their own responsibility for protecting corporate information. Attempting to impose security policies on unwilling people results in resistance both because more stringent security procedures make people's jobs harder, and because people do not like being told what to do—especially by security officials perceived as being outside the chain of command.

The only approach that works in the long run is to present security to everyone in the organization in a way that causes them to recognize that they, personally and professionally, have a stake in information protection. Security managers, to be successful, must involve employees from throughout the enterprise in developing security policies. Users must justifiably feel that they own their security procedures; employees with true involvement in the policy development process become partners rather than opponents of effective security.

46.3 PHASE 1: PRELIMINARY EVALUATION. Studies of the extent to which information security policies are in place consistently show that relatively few of the respondents have adequate policies in place. For example, the 2000 Global Security Survey run by *InformationWeek* and PricewaterhouseCoopers interviewed 4,900 executives, security professionals, and technology managers about their organization's security policies. According to the report, "only 38% of the respondents say their security policies are very well aligned with their business goals. Forty-five percent say their security policies are somewhat aligned with business goals, and 17% say the two don't mesh at all."[1] In other words, almost two-thirds of the organizations represented had inadequate security policies.

In what follows, it is assumed that a specific officer or manager (or group of officers or managers) in the enterprise have taken on the task of developing security policies. The group will be called the *policy development group.*

Before attempting to formulate policies, the policy development group needs formal authorization to use corporate resources in such a project. It should not be too difficult to obtain a short memorandum from top management to everyone in the organization that lays out the reasons for asking for their time and energy in gathering information about the current state of security. Such authorization and continuing top-level support are essential tools in convincing people to cooperate with the policy development group.

In the absence of existing or adequate security policies, a preliminary inventory is the first step in providing upper management with the baseline information that will justify developing a corporate information security policy. The preliminary evaluation should be quick and inexpensive—perhaps days of work by a few people. There is no point in wasting time in expensive detail work before getting approval, support, and budget from upper management.

The goal of the preliminary evaluation is to ask the people who work with information resources what they believe are their most important security needs. Even though they may not be conscious of security as a distinct need, in practice employees and managers do have valuable insights that transcend theory and generalizations. Data entry clerks may tell the security staff about security violations that no one else has observed or even thought about; for example, they may observe that a bug in a particular program makes the previous operator's data entry screen available for unauthorized entries when the shift changes and a new operator sits at the same terminal.

The policy development group should work closely with the human resources (HR) personnel in developing the research instruments for interviewing staff. The HR staff members are likely to know the key managers to contact in each department. The managers have to be convinced to support the effort so researchers can interview willing staff. Some of the HR people are likely to have the professional skills and experience required to provide accurate and cost-effective evaluations of beliefs, attitudes, and behavior affecting security. They may be able to help construct unbiased questionnaires, organize focus groups, and guide interviews.

However, if the security staff and the HR staff are not confident about being able to handle this preliminary data collection, the policy development group should see if it can obtain authorization to hire a consultant with proven expertise in collecting and analyzing social attitudes. The policy development group might want to discuss such a study with a firm specializing in security audits and organizational analysis. If no one knows where to start looking for such resources, the policy development group can contact information security associations, security magazines, security Web sites, and local universities and colleges to ask for suggestions.

The following key issues should be part of the preliminary study:

- Introduction to the study
- State of current policy
- Data classification
- Sensitive systems
- Critical systems
- Authenticity
- Exposure
- Human resources, management, and employee security awareness
- Physical security
- Software development security

- Computer operations security
- Data access controls
- Network and communications security
- Antimalware measures
- Backups, archives, and data destruction
- Business resumption planning and disaster recovery

The following sections suggest some typical questions that would be helpful in gathering baseline data about the current state of security. All these questions (and more site-specific topics) should be asked of all the respondents in the preliminary evaluation. Applicable questions are not necessarily repeated in each section; instead, questions in the earlier parts of this list may be adapted for use in later sections. These suggestions are not intended to limit creativity but rather to stimulate development of more questions that would be particularly useful for a specific enterprise.

46.3.1 Introduction to the Study. Employees may perceive many of the following questions as threatening. The preamble or introduction to the study, whether it is by survey or by interviews, should make it clear that this is not an audit or an attempt to punish people. The information should be anonymized so that no person will be targeted for reprisal if the study discovers problems. Every effort should be made to reassure employees that the study is designed to learn about the facts of security with a view to improvement rather than a search for culprits who will be punished.

46.3.2 State of Current Policy. The questions that follow not only gather baseline information about security policies but also determine whether employees have any idea about who is responsible for formulation of those policies.

- Does the enterprise have any security policies at all?
- Who developed them? An individual? A group?
- Where and how are the security policies available (paper, electronic)?
- When were the policies last updated? Last disseminated?
- Who, if anyone, has explicit responsibility for maintaining security policies?
- Who implements security policy at the enterprise level?
- To whom does the chief information security officer report within the enterprise?
- Who monitors compliance with security policies, standards, and compliance?

46.3.3 Data Classification. Questions to ask include:

- Are there levels of security classification that apply to your work? If so, what are they called?
- Are there rules for determining whether information you handle should be classified at a particular level of confidentiality?
- Are documents or files labeled to show their security classification?
- What is your opinion about the value of such classification?
- Do people in your group pay attention to security classifications?
- Do you have any suggestions for improvement of how data are classified?

46.3.4 Sensitive Systems. The questions in this section focus on information that ought to be controlled against unauthorized disclosure and dissemination.

- In your work, are there any kinds of information, documents, or systems that you feel should be protected against unauthorized disclosure? If so, name them.
- How do you personally protect sensitive information that you handle?
- How do others in your department deal with sensitive information? No names, please.
- To your knowledge, have there been any problems with release of sensitive information in your department?
- Do you have any suggestions for improving the handling of sensitive data in your area?

46.3.5 Critical Systems. The questions in this section focus on information that requires special attention to availability and correctness.

- In your work, are there any kinds of information, documents, or systems that you feel are so critical that they *must* be protected against unauthorized modification or destruction? If so, name them.
- Are there any special precautions you use or know of to safeguard critical data in your area?

46.3.6 Authenticity. Questions to ask include:

- Do you know of any cases in which anyone has used someone else's identity in sending out messages such as letters, faxes, or e-mail? If so, were there any consequences?
- Does anyone in your group use digital signatures on electronic documents?

- Does anyone in your group make or use unauthorized copies of proprietary software? If so, do you think there is any problem with that?

46.3.7 Exposure. Questions to ask include:

- What are the worst consequences you can realistically imagine that might result from publication of the most sensitive information you control in the newspapers?
- What might happen, in your opinion, if key competitors obtained specific confidential information that you use or control in your area?
- Can you estimate monetary costs associated with the scenarios you have described above?
- What would be the worst consequences you can foresee if critical information you work with were altered without authorization or through accidental modification?
- What might happen if you could not access critical information quickly enough for your work?
- Can you estimate the costs of such breaches of data integrity and data availability?
- Could there be trouble if someone forged documents in your name or in the enterprise's name? Can you sketch out some scenarios and associated costs resulting from such breaches of authenticity?

46.3.8 Human Resources, Management, and Employee Security Awareness. For additional ideas in framing questions about security awareness, see Chapter 29. For ideas on appropriate questions dealing with employment practices and policies, see Chapter 31.

- As far as you know, who is responsible for developing security policies?
- Do you know where to find the security policies that apply to your work?
- When, if ever, did you last sign any documents dealing with your agreement to security policies?
- Who is responsible for monitoring compliance with security policy in your work group? In the enterprise as a whole?
- Have you ever received any training in security policies? If so, when was the last time?
- Have you ever seen any written materials circulating in your work group that discuss information security?
- Do you think of protecting corporate information as one of your official responsibilities?

46.3.9 Physical Security. For more detail about physical security and additional ideas on appropriate questions, see Chapters 14 and 15.

- Does anyone check your identity when you enter the building where you work?
- Are there any electronic access-control systems limiting access to your work area? What are they?
- Do people hold a secured door open to let each other into your work area? Do you let people in after you open a secured door?
- Have you ever seen a secured door into your area that has been blocked open (e.g., for deliveries)?
- Do people leave your work area unlocked when everyone leaves?
- Do staff members wear identity badges at work? Are they supposed to? Do you wear your badge at work?
- Do visitors wear badges?
- Have you ever seen strangers in your area who are not wearing visitor badges?
- What would you do if you saw a stranger in your area who was not wearing a visitor's badge?
- Do you lock any parts of your desk when you leave your workspace?
- What would you do if you heard the fire alarm ring?
- Where is the nearest fire extinguisher?
- Who is the fire marshal for your floor?
- What would you do if someone needed emergency medical attention?
- Is there an emergency medical station in your area or on your floor?
- Do you know who is qualified in cardiopulmonary resuscitation (CPR) in your group or on your floor? Do such people wear identifying pins?
- Have you had recent training in what to do in the event of an emergency? Have you been trained in how to evacuate the building?
- Is there anything that comes to mind that you would like to see to improve physical security and safety in your work area?

46.3.10 Software Development Security. The following questions would be asked only of the software development team. For much more information suitable for devising questions about development security, see Chapter 25.

- Are there any security policies that apply to your work? What are they?
- Have you ever discussed security policies in your group?
- Is security viewed positively, neutrally, or negatively in your group? And by yourself?
- Do you and your colleagues discuss security during the requirements analysis and specification phases when developing software?
- How do you see quality assurance as part of the development process?
- Do you use automated software testing tools?
- Tell us about version control in your group. Do you use automated version control software?
- How do you document your systems?
- Do you think that your source code is adequately protected against unauthorized disclosure and modification?
- What is your opinion about Easter eggs (unauthorized code for an amusing picture or game)?
- Could anyone plant an Easter egg or a logic bomb (unauthorized, harmful functions) in code being developed in your group?
- Have you ever seen an Easter egg or a logic bomb in code from your group? Did it get through to production?
- Can you think of ways you would like to see better security in your work?

46.3.11 Computer Operations Security. The following questions would be asked only of the computer operations team. For more information suitable for devising questions about operations security, see Chapter 32.

- How long do you wait after initial release before installing new operating system versions on your production machines?
- How do you put new software into production?
- Can development personnel access production software? Production data?
- How do you handle problem reports? Do you have an automated trouble-ticket system?

- Can people from outside the operations group enter the operations center?
- Are contractors, including repair technicians, allowed to circulate in operations without being accompanied?
- Do cleaning staff ever circulate within the secured areas of operations without operations staff present?
- Are system components labeled?
- Is there an emergency cutoff switch for main power to the entire data center? Does it include air conditioning?
- Are there uninterruptible power supplies for critical components of your systems?
- Do you keep records of system downtime? What is your downtime over the last three months? The last year?
- What accounts for most of the downtime?
- Who monitors system resource utilization? Are there automated reports showing trends in disk space usage? CPU utilization? Network bandwidth usage?
- What improvements in security would you like to see in operations?

46.3.12 Data Access Controls. For additional ideas on looking at identification and authentication, see Chapter 16.

- Do you have to identify yourself to the computers and networks you work with?
- Do you have a user name (ID) that no one else shares?
- Are you required to use a password, passphrase, or personal identification number (PIN) as part of your routine when starting to use your computer?
- Have you ever shared your unique user ID and password or PIN with someone else? Or have you borrowed someone else's user ID and password to get some work done? If so, how often does this happen?
- Do you use a token, such as a physical key or a smart card, to prove who you are to the computer system? If so, have you ever lent or borrowed such tokens? What for? How often?
- In your work, are there any limitations on the data you are allowed to work with?
- Are there data you can see but not change?
- Do you use encryption on any of the data you work with?

- Do you or members of your group use laptop computers? If so, do you encrypt sensitive data on the disks of those portable systems?

- Do you or anyone in your group take work home? If so, do you put corporate data on your own, personal (noncompany) computers? Does anyone else have access to those computers? Are there any controls on accessing corporate data on the home computers?

46.3.13 Network and Communications Security. Most of the following questions would be appropriate only for network managers, administrators, and technicians. However, some of the questions are suitable for everyone. For more ideas to help in developing detailed technical questions, see Chapters 8, 17, 18, 19, 20, 21, and 22.

- As a user, do you know what the rules are about using your employer's e-mail system and Internet access?

- Do you know anyone who regularly violates system usage restrictions? No names, please.

- Have you ever seen pornography on corporate systems? Child pornography? Racist and other objectionable materials? If so, did you know what to do? And what did you do?

- Has anyone ever discussed rules for secure e-mail with you? Do you know how to encrypt sensitive messages? Do you ever encrypt messages?

- As a network manager, do you have up-to-date network diagrams, or can you produce them on demand?

- Do you know which services are running on your Internet-connected systems? Are all of the running services needed?

- How do you determine which patches are appropriate for installation on your systems? How often do you check? Who is responsible for managing patches? How long does it take between notification of a vulnerability and installation of an appropriate patch?

- Does your security architecture include firewalls? If so, what determines the security policies you instantiate in the filtering rules?

- Do you have egress filtering enabled on your firewalls?

- Do you have intrusion detection systems? If so, who responds to apprehended intrusions? How are the responsible people notified of an intrusion?

- What are the procedures for responding to an intrusion?

- If your organization uses passwords, how do you handle requests for new passwords?

- Do you have centralized remote-access controls?

- Do remote users use virtual private networks (VPNs) to access corporate systems from outside the firewalls?

- Are your users supposed to use encryption for sensitive e-mail that traverses the Internet? Do they? How do you know?

- Do your users apply digital signatures to all communications?

- Are your Web servers protected against intrusion and vandalism?

- Have you kept sensitive information off your Web servers?

- Do you encrypt all sensitive information stored on your Web servers?

- How long would it take you to recover a valid version of the Web site if it were destroyed or vandalized?

- Do your telephone voice-mail boxes have unique, nonstandard passwords? How do you know?

- How do you find out if an employee is being fired or has resigned? How long does it take between termination of employment of such an employee and deactivation of all system and network access?

46.3.14 Antimalware Measures. See Chapter24 for more ideas on checking for appropriate levels of antimalware precautions.

- Do you and all of your users have antimalware products installed on every workstation?

- How often are antimalware products updated? How are they updated?

- How long does it take for all vulnerable systems to be brought up to date?

- Do you or your users open unexpected, unsolicited e-mail attachments?

46.3.15 Backups, Archives, and Data Destruction. For additional suggestions to help in framing questions about data backups, see Chapter 41.

- How often do you do backups of your electronic data?

- Where do you store backup media? Are current copies retained off site as well as on? How do you know which media to use to restore a specific file?

- How long do you keep different types of backups? Why?

- How do you prevent unauthorized access to backup media?

- If you keep data backups for several years, how do you ensure that the old media will be readable and that the data developed for old applications will be usable?

- How do you dispose of magnetic and optical storage media after their useful life is over? Are the discarded media readable?

- Do you make backup copies of paper documents? Where are these copies kept? How would you locate a specific document you needed?

- How long do you keep various types of papers? Why?

- When you dispose of paper documents, does their content influence how they are destroyed? How do you dispose of sensitive paper documents?

46.3.16 Business Resumption Planning and Disaster Recovery. For more ideas on questions that are appropriate in quickly evaluating the state of business resumption planning and disaster recovery, see Chapters 42 and 43.

- Do you have business resumption planning (BRP) or disaster recovery plans (DRP)? If so, where are they kept?

- Who is responsible for keeping BRP and DRP up to date?

- Have you ever participated in a BRP or DRP testing? If so, how long ago was the last one? When is the next scheduled test?

- During BRP and DRP tests, does anyone use movie cameras or tape recorders to keep track of critical steps in the recovery?

- After a test, have you participated in analyzing the results of the tests to improve the plans?

46.4 PHASE 2: MANAGEMENT SENSITIZATION. Support from upper management is essential for further progress. The goal in this phase is to get approval for an organization-wide audit and policy formulation project. In conjunction with the rest of the information security project team, the responsible managers should plan on a meeting that lasts no more than one or two hours. The meeting should start with a short statement from a senior executive about the crucial role of information in the organization's business.

Professional aids such as management-oriented training videos are helpful to sensitize the managers to the consequences of poor information security. For an up-to-date list of such videos, enter the keywords “information security training video” into a search engine such as Google.[2] After the video film, the team can present its findings from the preliminary evaluation. The immediate goal is to constitute an *information protection working group* to set priorities, determine an action plan, define a timetable and milestones, and formulate policies and procedures to protect corporate information resources. The presenters should name the people

you want to see on your working group; all of these people should be contacted before the meeting to be sure that they have agreed in advance to participate in the working group.

The presenters should provide estimates of the time involved and the costs of in-house, and consulting, services and software. To end the briefing, it is useful to offer upper managers a range of background reading about security; Appendix A2 on the Internet at www.XXXXX.com has suggestions for such readings. Some managers may be intrigued by this field; the more they learn, the more they will support security efforts.

46.5 PHASE 3: NEEDS ANALYSIS. The information protection working group should include representatives from every sector of the enterprise. As the group investigates security requirements, the participants' wide experience and perspective will be crucial in deciding which areas to protect most strongly. More important, their involvement is a concrete expression of corporate commitment to a fundamental attitude change in the corporate culture: Security is to be an integral part of the corporate mission.

For example, in a manufacturing firm, the team would include managers and staff from the factory floor, the unions, engineering, equipment maintenance, shipping and receiving, facilities management (including those responsible for physical security), administrative support, sales, marketing, accounting, personnel, the legal department, and information systems. Each of these members of the working group will help improve enterprise security.

If the organization is very large, the group may have to set up subcommittees to deal with specific sectors. Each subcommittee evaluates to what degree the systems and networks are vulnerable to breaches of security. For example, one group could focus on local and campus communications, another on wide area enterprise networks, and a third on electronic data interchange with clients and suppliers.

A typical audit covers the facilities, personnel policies, existing security, application systems, and legal responsibility to stakeholders (owners, shareholders, employees, clients, and the surrounding community). Based on the findings, the subcommittees formulate proposals for improving security. This is where the specialized knowledge obtained from information security specialists and information security courses will prove especially useful.

Chapters 36, 45, and 47 have information that will help the information protection working group develop an evaluation plan. In addition, the National Institute of Standards and Technology has published the *Guide for Selecting Automated Risk Analysis Tools*[3]; risk analysis tools can help practitioners speed up the evaluation process in this phase of the policy development process.

46.6 PHASE 4: POLICIES AND PROCEDURES. Once the information protection working group have built a solid floor of understanding of enterprise information security needs, they are ready to construct the policies and procedures that meet those needs. Chapter 28 contains many suggestions and resources for the content and style of security policies. The process should start from existing templates and normally takes weeks to months to complete a workable draft.

Genuine participation by all the representatives from every sector of the enterprise is a critical element of success; without a thoroughgoing sense of ownership of the policies, working group

members will fail to internalize the new policies. All the members of the working group must become enthusiasts for their collective efforts; in some sense, these people become missionaries engaged in the long-term conversion efforts of phase 5, the implementation of the policies.

46.7 PHASE 5: IMPLEMENTATION. Once the working group members have defined the new or improved security policies, they are about halfway to their goal. The hardest part is ahead: explaining the need for security and the value of the new policies to fellow employees and convincing them to change. Even if they agree intellectually, there is a good chance that their ingrained social habits will override the new rules for at least months and possibly years. The challenge is to overcome these habits.

Chapter 35 shows in detail how to use the insights of social psychology to change corporate culture by working on beliefs, attitudes, and behavior. In addition to the suggestions in that chapter, the information protection working group should organize and deliver awareness and training sessions for all levels of the enterprise:

- Upper management
- Technical support
- Lower-level staff
- Other technical staff.

The following sections offer some simple agendas for such preliminary sessions.

46.7.1 Upper Management. Security policies and procedures require management support and sanctions. The transformation of corporate culture should begin at the top. Although it is difficult to coordinate the presence of top executives, the working group should try to organize a half-day executive briefing session on enterprise security. In practice, the group may be able to convince upper management to attend for one or two hours. The focus should be intensely practical and show executives how to protect themselves and the enterprise against common dangers. Suggested topics:

- A review of the business case for improving security: industrial espionage, natural and man-made disasters, vandalism
- Network security: protection against eavesdropping and tampering
- Access controls: tokens, biometrics, passwords
- Encryption: e-mail, laptops, provision for emergency data recovery
- Backup policies for PCs, networks, and mainframes
- Security agreements: summaries of the policies and procedures to be read and signed annually

- Need for total support to convince other staff to comply with security policies

46.7.2 Technical Support. The next target is the technical support group, the people who help explain security policies to users. In a one-day training session, the presentations can cover

- Everything covered in the executive briefing
- Operating system security provisions
- Security software features
- Changes in operations to comply with new procedures

46.7.3 Lower-level Staff. Lower-level staff need a half-day session that answers the following questions in terms that apply directly to their own work:

- Why should I care about information security?
- What are my obligations as an employee?
- How do I protect the PC I am responsible for against viruses?
- How do I back up my data?
- How do I manage my passwords?
- What must I do if I see someone violating our security policies?

The class ends with participants signing the security agreement.

46.7.4 Other Technical Staff. More intensive training and education are needed for technical staff, such as members of the software development, operations, and network administration groups. More in-depth, specific material will have to be incorporated into their training; however, such training can be spread over a longer time than that for the groups already discussed because of the rhythm of work and the crucial importance of technical competence for implementation of the policies. Most enterprises rely on outside trainers, specialized off-site or online courses, and certification programs to raise their staff to the appropriate levels of competence.

46.8 PHASE 6: MAINTENANCE. Once the enterprise has begun to integrate a concern for security into every aspect of its work, the issue must be kept fresh and interesting. As described in Chapter 29, successful security awareness programs include amusing posters, interesting videos, occasional seminars on stimulating security topics such as recent frauds or computer crimes, and regular newsletters with up-to-date information. Finally, every employee should regularly reread and sign the annual security agreement. This practice ensures that no one can argue that the organization's commitment to security is a superficial charade.

46.9 CONCLUSION. For a secure installation, three things are essential:

1. Sound policies that have been developed with the cooperation of everyone concerned and that are updated periodically

2. Widespread dissemination of those policies, with ongoing observation of their implementation, and with frequent training and continual reinforcement

3. Commitment to security on the part of everyone, from top management on down

When these essential elements are in place, the entire organization will function at a more productive level, one at which the possibilities of disruption and damage will have been reduced to a minimum. Nothing less is acceptable.

END NOTES

[1] See *www.informationweek.com/794/security.htm.*

[2] *www.google.com.*

[3] *csrc.nist.gov/publications/nistpubs/500-174/sp174.txt.*

