A Guide to Security Policy

A Primer for Developing an Effective Policy

RSA SECURITY™

Table of Contents

INTRODUCTION

As computer networks become more complex and corporate resources become more distributed, the need for improved information security is increasing. While most organizations begin by deploying a number of individual security technologies to counteract specific threats, the adoption of the Internet as the foundation for e-business has turned security into an enabling technology that is required for business success.

At some point there becomes a clear need to tie together the techniques and technologies that both protect and enable your business through security policy — a thoughtful and consistent management approach to security practices across the organization. RSA Security has nearly twenty years' experience implementing security solutions, from developing highly secure products to developing policy to deploying the two together. It is that experience and expertise that has led to this guide — to help you develop your own effective security practices. We know the questions you need to ask yourself.

If you are reading this guide, you probably already recognize the need for a consistent approach to information security. This guide is intended to be the first step, giving you an overview of the decision-making process necessary to develop an effective security policy for your company.

Specifically, *A Guide to Security Policy* provides information about:

▶ The need for information security

▶ The process of developing an effective security policy

▶ Implementing your security policy

▶ Information about what other companies are doing

Your actual policy-making journey will involve classifying the corporate information you want to protect, identifying potential security threats and business risks, and deciding what levels of protection will make it possible to do business online. While "airtight" information security across the organization may be your goal starting out, in reality you will be balancing security levels with their costs, as well as with your business practices and corporate culture. The written policy document you come up with will reflect the difficult decisions you make during this process regarding information access, corporate strategy, resource allocation and employee behavior.

And it will never really be "finished": your security policy will essentially become a dynamic insurance policy that you will modify regularly to keep pace with changes in technology and your business practices. However, by creating a security policy for your organization, you are taking an important step toward elevating your information security practices so your organization can prosper in today's evolving e-business world.

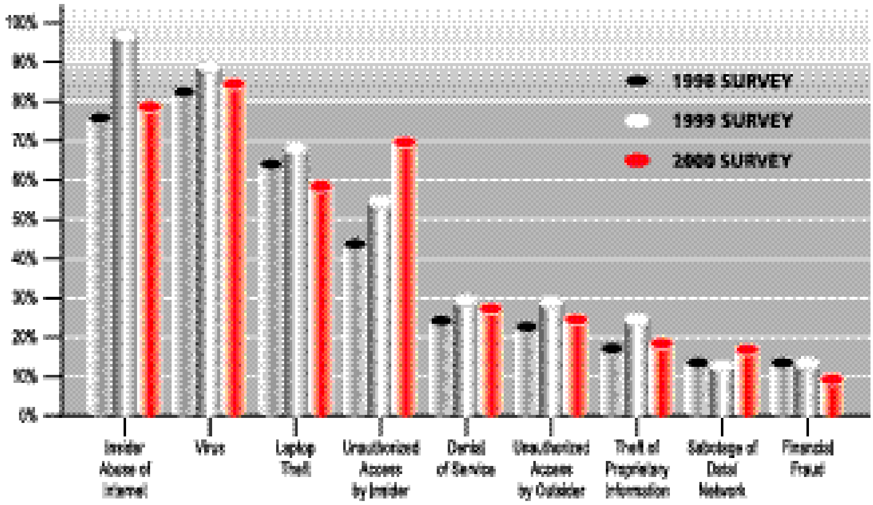
WHY YOU NEED A SECURITY POLICY

The essence of security policy is to establish standards and guidelines for accessing your corporate information and application programs. Typically, organizations start with informal and undocumented security policies and procedures; but as your enterprise grows and your workforce becomes more mobile and diverse, it becomes especially important — even necessary — for your security policies to be documented in writing. Doing so will help avoid misunderstandings and will ensure that employees and contractors know how to behave. It will provide explicit guidelines for your security staff, making it easier for them to enforce security policies consistently. Furthermore, a security policy facilitates internal discussion about security, and helps everyone become more aware of potential security threats and associated business risks. You'll find that a written policy generally tends to enhance the performance of your security systems — and the e-business applications they support. It provides the guidelines necessary in determining the proper configuration of systems and a bar against which you can measure the effectiveness of your security efforts. A deciding consideration is that having a written security policy may be required by law.

The need for security is increasingly obvious

Since 1996 the Computer Security Institute, in conjunction with the FBI, has conducted an annual survey to monitor computer crime trends. This research project is one of the few that provides benchmark readings of information security issues from year-to-year. Some of the key points from the most recent (2000) survey include:

- **Most organizations surveyed have been victims of computer crime.** 90% of respondents admitted that they had been victimized by computer security breaches in the previous 12 months, compared to 62% in the 1999 survey and 64% in the 1998 survey. When considered in light of the fact that many, if not most computer crimes go undetected, it is clear that the issue of security breaches should be of concern to every organization.
- **Computer crime causes significant damage.** Not all organizations that were victimized by computer security breaches were able to quantify their losses. However, the losses of the 42% of survey respondents that could totaled $265,589,940. Notably, the theft of proprietary information resulted in the highest financial losses, continuing a rising trend, followed by financial fraud.
- **Computer crime is increasing.** The problem of information security is not limited to the United States; in fact, many of the crimes reported in the CSI/FBI research originated outside the United States. A quick review of press reports shows that information security is a problem for organizations the world over — Japan, China, India, Russia, Europe and Latin America. Simply put, as the use of computing increases in a society, so grows the risk of information crime.



The 2000 CSI/FBI Computer Crime and Security Survey

- **Insiders pose as significant a threat as outsiders.** It is common to think of security in terms of protecting network perimeters from hostile outsiders attempting to gain access. But inappropriate insider behavior can be a bigger threat, both more common and often causing greater financial losses than outsider attacks. The 2000 survey reports that 71% of respondents detected unauthorized access by insiders. In addition, simple abuse of Internet access privileges — which affected the majority of companies in the CSI/FBI study — costs the enterprise money in terms of reduced productivity and wasted network bandwidth.

There are many costs associated with security breaches

- **Direct financial loss.** Customers' credit card numbers, the company's merchant account passwords, and employees' personal checking account numbers are all prime targets for thieves. And whether or not the criminal is brought to justice, indirect legal fees or fines resulting from the crime can add significantly to the costs, especially in industries like banking and finance.
- **Lost sales and reduced competitive advantage.** When proprietary sales proposals, business plans, product designs or other information are stolen, altered or destroyed, it can give competitors a distinct advantage. Lost sales can result, and the impact can be felt long after the incident occurs.
- **Damage to your corporate reputation and brand.** You work hard to build and maintain your corporate image and to establish trusted relationships with your customers and business partners. If proprietary or private information is compromised, your corporate credibility and business relationships can be severely damaged.

- **Privacy violation.** Employees trust you to keep their personal information private. Similarly, customers trust you to keep their credit card numbers and credit histories confidential. If that privacy is violated, legal and other consequences can result.
- **Business disruption.** When a service disruption occurs, your IT staff needs to address the problem immediately. Hopefully, they'll be able to restore data from backup files, and return systems to service without significant downtime. However, in the case of mission critical systems, any downtime can be catastrophic. And other times, lost data may have to be painstakingly reconstructed by manual means, prolonging the time that systems are functioning below acceptable levels.

A security policy mitigates your legal exposure

Your security policy guides the behavior of your employees and ensures that they know what you expect of them. Having a written policy is mandatory if you expect to be able hold them accountable for their actions. In many countries around the world, CEOs and senior management may be legally responsible for crimes involving their organization. Punishment can include both fines and imprisonment. To avoid this liability, corporations generally need to be able to prove a "good faith" effort to deter criminal activity that utilizes their computer systems and networks. A comprehensive security policy will help reduce this exposure — it is expected to include written policies and procedures to deter crime, security awareness programs, disciplinary standards, monitoring systems consistent with current industry practices, and immediate reporting of any detected crimes to law enforcement agencies.

Note that in the United States, good faith guidelines no longer consider simple password-only user identification schemes to be adequate. Two-factor authentication, consisting of something you know (a password or PIN) plus something you possess (a physical authenticator), is now considered the industry norm when evaluating the effectiveness of a security program. Under U.S. Federal Sentencing Guidelines, an organization's culpability is lessened by having an effective program to detect and prevent security violations.

In other countries the rules relating to computer security may be even more strict. For example, in China the government has extremely demanding regulations relating to encryption, which prevents some common software from being used in China. An organization that transcends borders can use a policy to help maintain legal security practices that differ from country to country.

A security policy forces you to make return-on-investment decisions

Security threats have the potential to exploit a vulnerability in your organization's computer practices, with the potential for damaging your information assets. The threats you identify will run the gamut from natural disasters to malicious hackers penetrating your network. Your job in developing a security policy will be to make intelligent business decisions about the cost-effectiveness of reducing or eliminating each of the threats — and to base your decisions not on the fact the threat exists, but rather on the associated risks to your business. We'll discuss this assessment process further in a subsequent section.

DEVELOPING AN EFFECTIVE SECURITY POLICY

The process for developing a written security policy typically involves a task force with representatives from a variety of functional groups. Be sure to include some “business” people, and not just IT, engineering and security staff. These business people – whether sales, finance or operations – will ensure that the policy you develop supports business practices rather than hinder them. Ultimately, it will be very important for you to get senior management involved, and to get the CEO to endorse your security policy. Upper management needs to send a clear message to everyone in the organization that information security is vitally important to the company.

During this process, keep in mind that your security policy can’t be so strict that it incapacitates your business. And it needs to be enforceable; otherwise, your employees will ignore it. Also consider the role of outsiders — contractors and business partners may require access to your information assets. Your task force’s initial job will be to assess security threats to your organization’s information assets with respect to each of the following fundamental areas:

- Authentication — ensuring that a user is who he says he is.
- Authorization — controlling what information and applications a user can access.
- Privacy and data integrity — preventing unauthorized users from seeing certain information, and preventing them from making unauthorized changes or deletions.
- Non-repudiation — making sure that parties in a transaction can’t deny what they said or what they did.
- Disaster recovery & contingency planning
- Physical security

As the security task force makes decisions relating to the above security topics, it will also need to balance four distinct business factors:

- the information access requirements of different constituencies, both inside and outside your company,
- the value of the information stored,
- the liability of the transactions available, and
- the budgetary impact of implementing that security — both the initial costs and the recurring costs, like staff time.

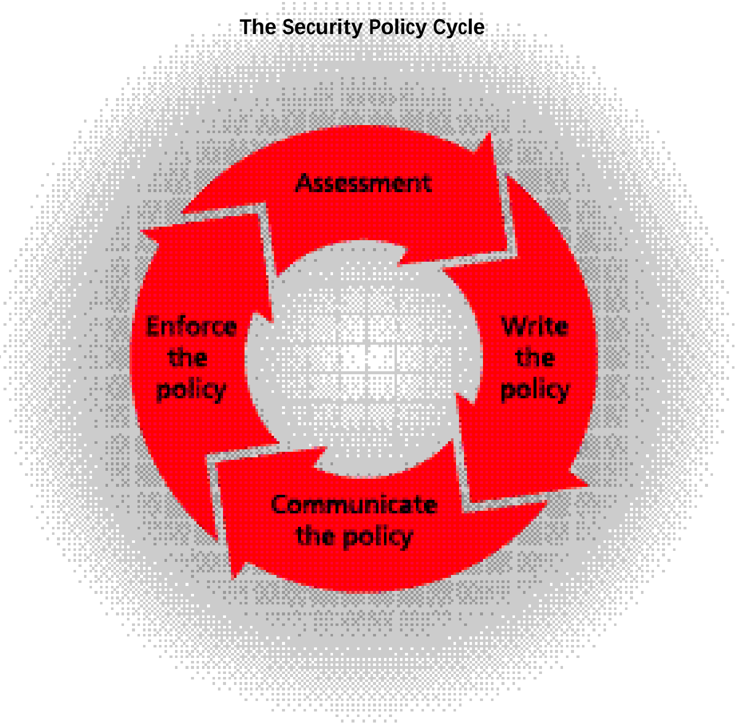
Obviously, it can be a difficult task to establish a policy that meets your desired security goals and your budget constraints, and is acceptable to all users. It is important to get the right people on your policy-making task force. After assessing user access needs, business risks, security threats and protection costs, this team will need to make objective ROI-based decisions based on tradeoffs between risks and costs.

Having a written security policy in place, however, is just the first step. You will need to effectively communicate that policy to employees, contractors and others. And your staff will need to enforce the policy. Enforcement will involve managing access control lists and authentication systems, monitoring networks and computer systems for possible security breaches, and reacting appropriately when security violations occur. You should also reevaluate your policy on a regular basis, as changes in technology and business practices uncover new threats or reveal new online business opportunities.

In the rest of this section we will provide some guidelines that should help you organize the security policy-making process. The general sequence of steps your security task force will follow will be:

- **Assess requirements** — understand information assets, user access requirements, business risks, security threats, protection techniques and ROI.
- **Write the security policy**
- **Implement the security policy** — communicate it, enforce it consistently, and reassess it regularly to address new security threats and take advantage of new protection tools.

The Security Policy Cycle



ASSESS SECURITY REQUIREMENTS

Assessing computer security risks is about categorizing information assets, business risks, user needs, security threats, and protection tools and techniques, so that you can make rational decisions based on the return-on-investment for various levels of security implementation.

Cover your assets

The first step in assessing security risks is to take stock of your enterprise's information assets — application programs, stored communications, reports, product designs and specifications, proposals, business plans, financial records, databases, and other files and documents residing on your organization's computer systems. Your objective is to organize these assets, conceptually, into appropriate categories, to help you understand them and their boundaries. You need to determine the appropriate owners of the various assets and convince them to take responsibility for evaluating their importance and value.

There are a variety of classification schemes you can consider as you organize your information assets:

- **Geography** — plants, buildings, remote sales offices.
- **Group** — manufacturing, engineering, marketing, customer support, accounting, administration.
- **Who manages the computer system** — the engineering systems, the HR network, the Web and intranet servers.
- **Technology** — Windows NT, Windows 98, Mac, UNIX, mainframe, TCP/IP, Token-ring, AppleTalk.
- **Product development cycle** — R&D, QA, production.
- **External or internal** — Web site, extranet, intranet, internal network.

Once you have identified the information resources and developed appropriate ways of classifying and understanding their perimeters, the next step is to define who needs access to what information.

Define access requirements

Now that you understand what you're trying to protect, you need to categorize users according to what information they require in order to do their jobs. For example, management needs access to strategic plans and legal documents, but manufacturing personnel typically don't need to see that information. Similarly, order entry and accounts receivable staff need to view customer orders and credit card numbers; other staff don't. You could define a spreadsheet matrix to classify which users need access to each asset, similar to the one on the following page.

Access required by users (1=highest need):

Asset	Mktg	Sales	Admin	Mfg	Supp	R&D	QA	IT
Sales database	1	1			2			1
Product drawings	3			1	1	1	1	1
Product specifications	2	2		1	1	1	1	1
Order database	2	1	1	2			1	
Web site	1		2		2			1

Once you understand how users access information, you will need to evaluate each asset's relative importance, and the risks associated with its being stolen, damaged or destroyed. Note that the "owner" of the information has the final say as to the value of that information. The value of information assets may even be dynamic, changing weekly, daily or even hourly.

Analyze security threats

You're now ready to ascertain the areas of vulnerability for your network and computing platforms. During this phase many companies elect to get an outside security consultant involved, in order to get an expert assessment of specific security threats for their computer systems and networks. You may find it useful to think in terms of whether the threats originate inside or outside your organization, or both; keep in mind that research shows that insiders are as a serious threat as outsiders — if not more so.

Common threats to information security include social engineering, password cracking, network monitoring, abuse of administrative tools, man in the middle, denial of service, trojan horse, virus and address spoofing. Details on these common threats are available in RSA Security's publication, A Guide to Security Technologies.

Blindly applying technology to protect against every conceivable threat is not the smartest way to deal with security. A better way is to identify how much business risk each threat poses — how vulnerable are you, really, if a particular threat occurs? This way of thinking helps you minimize security implementation costs, and provides the flexibility you'll need to help you evaluate new threats. By considering the business risks, as well as the out-of-pocket expenses and time required to fix each new vulnerability, you'll be able to make an intelligent business decision about whether it makes sense to mitigate the threat. Note that your exposure is proportional to how long it takes to fix the problem, multiplied by the level of risk involved.

Identify business risks

The risks to your business were covered previously, and include direct financial loss, lost sales and reduced competitive advantage, damage to your corporate reputation and brand, privacy violation and business disruption. As part of your risk analysis, you may want to quantify the business risks in terms of expected, worst-case and best-case scenarios to assist in your decision-making process.

For example, if all of your confidential customer records are stolen, you could logically conclude that there will be direct financial costs, some lost sales, legal and PR costs, staff time to fix the problem, and security improvements. Knowing how many customers you have, and estimating the various business costs, you might estimate the worst case scenario to cost your company up to $5M, the expected scenario to cost you $500K, and the best case still to cost $100K.

As another example, if your sales prospect database is stolen, you might define the worst case scenario as losing all of the expected sales to those prospects, the expected case as losing 50% of expected sales, and the best case as losing 20% of the sales. Note that as part of this analysis, you'd need to decide upon the value of a typical sale, and factor in the percentage of prospects that actually become customers. The point in doing this analysis is to assign numbers to each of the perceived risks, so you can make some decisions about their relative importance.

You could define a spreadsheet to assist in this process, estimating the business costs associated with each of your assets. You might define risk factors for the best-case and worst-case scenarios, which get applied to your expected costs, such as:

Risk factor:	500%	100%	20%		Expected cost ($000):				
Asset	Worst case	Expect	Best case		Direct $ loss	Comp loss	Lost sales	Legal	Staff time
Prospect database	$600	$120	$24	=	$0	$20	$50	$20	$30
Product drawings	$1000	$200	$40	=	$0	$50	$50	$0	$100
Product specs	$850	$170	$34	=	$0	$50	$40	$0	$80
Order database	$2425	$485	$97	=	$300	$10	$50	$50	$75
Web site	$350	$70	$14	=	$0	$30	$10	$10	$20

Investigate new business opportunities

As you assess your requirements, keep in mind that security isn't just about threats and risks. For example, there are a number of strategic e-business opportunities that just wouldn't be practical without adequate information security. Secure Sockets Layer (SSL) encryption and digital certificates prevent sensitive information from being compromised as it passes between Internet clients and servers. These technologies let your customers order products and services safely, directly from your Web site. Similarly, these tools and others give you the ability to develop a supplier extranet that will let your purchasing agents issue purchase orders and track incoming orders online, saving them time and improving your just-in-time inventory availability. And an encrypted Virtual Private Network (VPN) can make sensitive price lists, sales reports and competitive insights available 24/7 to your authorized sales representatives around the world. All of these e-business opportunities are feasible because of information security.

Explore protection and enablement options

Once you define the business opportunities, in addition to the risks and threats, you can look at tools and techniques for protecting your information assets and enabling e-business. Various security options are available that address how to:

- Verify that users are who they say they are.
- Control access to data and functions.
- Protect the privacy and integrity of information assets.
- Ensure non-repudiation, so parties in a transaction can't deny their actions.

Authentication. A fundamental security requirement, authentication requires users to prove they are who they say they are. The most basic approach is to require users to provide information that, presumably, only they know, such as a username and password, their mother's maiden name, or a PIN number. A second approach is to use something they possess to present proof, such as a dedicated authenticator or smart card, special authentication software or a digital certificate. Still another approach to authentication utilizes biometrics — fingerprints, voice prints, retinal scans, etc. Two-factor authentication, which utilizes two of these approaches (e.g. password and authenticator), is generally considered the optimum way to ensure an adequate level of security.

Authorization. Used for access control purposes, identification involves issuing entry privileges only to those individuals who require access to specific information or applications. There are various systems for access control in both LAN and Internet environments, and there is a growing demand for single, or reduced sign-on requirements to minimize the number of times that authorized users need to authenticate themselves.

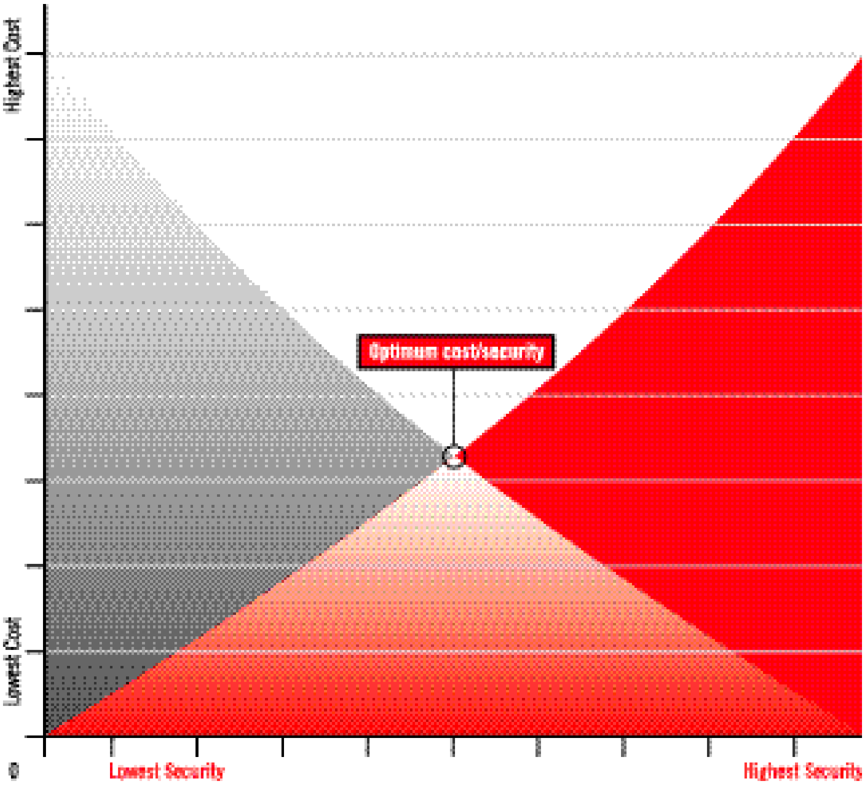
Data privacy and integrity. This issue involves preventing users from eavesdropping, viewing, tampering with or otherwise accessing unauthorized information. The most common approach to this problem involves encryption, which makes information unintelligible to unauthorized users and provides an indication of any tampering. A common example of data privacy involves encrypting customers' credit card information when it is sent from their PC to a Web server.

Non-repudiation. Preventing parties in a transaction from later denying things they said or did is an increasingly common requirement for e-business. Security tools designed to address this problem can provide proof that 1) a message or order wasn't sent by an imposter, and 2) the intended addressee actually received the information.

Physical security. Limiting physical access to servers, routers and other systems is obviously a good idea. In a similar vein, by physically reorganizing or consolidating information assets, you can simplify the management of those assets while increasing their security. For example, moving the customer and order databases to their own server makes it easier to control access and manage those specific assets.

Evaluate return on investment (ROI)

Knowing the threats to your information and your options for mitigating those threats, you now need to evaluate the return on your security investment, balancing protection costs against your business risk costs. Complete protection will not be feasible. An appropriate level of security involves implementing enough protection so as to minimize your business risks, similar to the following graph:



As part of your ROI analysis, you may decide that the cost of implementing a solution to a particular threat outweighs your worst-case exposure. In that case, it obviously doesn't make good business sense to address that particular threat. For example, it may not worth investing in biometric authentication for access to your corporate intranet, since its information is intended for all employees, is not especially confidential, and the business risks of information loss or damage are relatively minimal.

WRITE THE SECURITY POLICY

Once you've assessed your security requirements and understand the return on investment (ROI) issues, it's time to draft your security policy. Typical security policies address most of the following topics. There may be some overlap between your "security" policy and your "general" computer usage policy. You'll notice that some of the topics mentioned in this section, such as prohibiting employees from making copies of commercial software for personal use, aren't strictly security-related. But they are an important part of establishing a "do the right thing" mind-set among your computer users and mitigate your legal exposure.

Cover letter. A letter from the CEO will emphasize and reinforce the fact that security is vitally important to your organization.

Purpose. This section is typically a general overview or "mission statement" for the security policy document that explains its goals, to whom it applies, to what information and equipment it applies, and the underlying business reasons for having a security policy.

Responsibilities and authority. Your security policy should clearly define the responsibilities for developing and enforcing the policy. This will typically include defining who is responsible for reviewing and approving the policy (probably an information security committee), for establishing and maintaining the policy (possibly a director of security), and for administering the security policy (typically IT staff and system administrators). In addition to defining everyone's roles, this section could indicate that department managers are responsible for ensuring that their staff understand and adhere to the security policy.

Definitions. It's useful to define the technical terms used in the security policy document for non-technical readers; this may take the form of a glossary of terms at the end of the security policy document.

Information ownership and access rights. This will be a general statement defining the ownership and access rights for the information stored on your computers or transmitted via your network. You may want to relate this policy to related HR policies. The intent is to let your employees know that you have the right to monitor their e-mail or files, should you so choose.

Computer system usage. This section defines the primary purpose of your company's computer systems as being for your business purposes only. It may stipulate whether your employees can utilize your computers and network infrastructure for personal use, and the conditions under which they may do so. A general statement about user accountability is appropriate for this section, to make employees aware that they are fully responsible for maintaining the secrecy of their user ID and password, as well as all other proprietary company information, and possession of any security devices, such as authentication devices and smart cards.

Access control. This section should include information about the administrative controls and procedures for providing access to your company's computer systems and networks. The access control section will typically discuss the following points:

- **Identification and authentication.** Users will need at least a valid user ID and password to gain access to your network. You may choose to restrict access to standalone, non-networked computers in a similar way. Strong, or two-factor authentication — e.g., tokens or smart cards in addition to a user ID and password — has become the requisite protection for "sensitive" information and systems. You should identify which of your users need access to sensitive information and systems, and will need to use strong authentication.

- **Keeping user IDs and passwords secure.** This section should discuss basic guidelines for keeping users' IDs and passwords secure, such as how to choose a "good" password (e.g. six to twelve characters, mixed upper and lowercase, includes numbers, doesn't have any personal information, doesn't consist of a dictionary word, isn't descriptive of their work activity, etc.), never sharing or revealing a user name or password, and not storing unencrypted passwords on computer media.

- **Account administration.** Someone — typically authorized security staff, system administrators or IT staff — will need to assign and maintain login accounts, work group privileges, e-mail addresses, any authentication devices and digital certificates across a variety of computer systems and networks.

- **Privileged access.** You will need rules about who gets "root," "super-user" or "admin" access to your computer systems. Generally, this privileged access should be reserved strictly for the system administrator.

- **Access by non-company personnel.** If contractors, customers or vendors will be allowed to access your computer systems and network, you will need to define the conditions for their access.

- **Remote access and telecommuting.** You should define who will be permitted to access your computer network remotely. Department managers are usually responsible for authorizing remote access for telecommuting workers, sales personnel and others with a valid business need. Staff requirements for remote access should be reviewed on a regular basis. You will also need to define how remote users gain access to your networks — for example, by dialing in to a dedicated security server, but not by direct modem access to any individual desktop computer on your network. If appropriate, you should emphasize the importance of user authentication for remote access, and make people aware that an audit trail will be recorded for their remote access sessions.

- **Unattended computers.** When users walk away from their desks, their logged-on computer presents a network security risk. Discuss any requirements for logging off the network when users leave their desk, or for using software that will prevent access (by blanking the screen and/or locking the keyboard) if a user's computer remains idle for some period of time.

- **Unauthorized computers.** Many users own personal computers. You should define the circumstances under which users are permitted to bring personal computers into the office, and the conditions under which they can connect them to your network.

- **Non-network connections.** It's generally not a good idea to allow non-network communications (direct modem access) between individual computers on your network. And especially not with computers outside of your company.
- **Non-networked computers.** All standalone computers should have appropriate access controls.

Electronic mail. You need to emphasize to users that e-mail makes it all too easy to make your proprietary corporate information visible to the public. Your general e-mail policy should clearly state what's permissible content. In addition to not sharing sensitive corporate information, you should probably ban messages which contain threats, racial slurs, sexual harassment or which circulate chain letters. Some specific e-mail security issues include:

- **Privacy.** Emphasize that corporate information needs to be kept private, and that employees are not permitted to access or share information that doesn't relate to their jobs. Discuss the fact that sensitive corporate information should be encrypted to ensure privacy while the information is in transit.
- **Message encryption.** Discuss the specific e-mail encryption tools and techniques which you recommend or require, including guidelines for managing public and private encryption keys.
- **Monitoring.** As mentioned above, you should point out to employees that their e-mail messages are corporate information, and that they may be scrutinized by corporate management. Discuss any restrictions on employees using your corporate e-mail capabilities to communicate with family and friends outside your organization.
- **Message forwarding.** You should advise users to exercise caution when forwarding e-mail messages that may contain sensitive corporate information which should only be viewed by certain people. You might want to place restrictions on forwarding internal messages to outsiders, and to prohibit bulk e-mailings.
- **Message archiving.** Received e-mail messages tend to accumulate and take up valuable storage space. You may want to define rules for when users' un-needed messages should be purged, and what their responsibilities are in this area. Will old messages be deleted automatically, or do users need to manage this process? It would be appropriate to define your corporate backup policies with respect to users' archived messages.

Laptops, notebooks and handhelds. Portable computers designed for use by mobile professionals present some unique issues, and require both physical and electronic security precautions. You should discuss the responsibilities of portable computer users, including what happens when their portable computer is lost or stolen. Specific security issues include:

- **Theft prevention.** You may want to suggest techniques for preventing theft, such as using a locking cable and/or an alarm, and never leaving portable computers unattended.
- **Identification.** You should use inventory control labels or engraved markings to identify portable devices as being the property of your company. You should define who will maintain the inventory records for portable devices, especially if these devices are shared by multiple people.

- **Property checkout procedures.** You may want to have a checkout policy in place for devices which are shared among multiple people, or which employees remove from your facilities.
- **Loss or theft reporting.** If a portable device is lost or stolen, the user needs to report that fact promptly.
- **Access control.** Since sensitive information will likely reside on the portable computer, you may want to require access control software, so that users have to enter a user ID and password — or two-factor tokencode — in order to use the system. It may also be a good idea to require use of a screen saver that blanks the screen and requires users to reenter their ID and password whenever the system has been idle for awhile. As part of the property check-out process, security staff may need to configure each portable device's user ID, password and screen saver.
- **Preventing unauthorized observation.** With improvements in the viewing angles of computer displays, you should caution users to shield their portable devices from the curious eyes of airline passengers in neighboring seats.
- **File encryption.** To protect sensitive information on portable computers, even if they are stolen, you may want to require encryption software to be installed and used on these devices.
- **Virus detection.** Since portable computers are somewhat more likely to be exposed to computer viruses, it's appropriate to require virus detection software to be installed, properly configured and updated regularly.

Returning leased equipment. From time to time employees may need to lease equipment that stores information (such as a laptop computer). You should make employees aware that they need to remove any sensitive information (sales presentations, price lists, business plans), from the leased equipment prior to returning it. You may need to define guidelines for how to delete files so as to prevent their contents from being recovered.

Equipment repairs. Computers do fail, and sometimes need to be sent to an outside vendor for repair. You may want to require users to encrypt any sensitive files to minimize the possibly that outsiders can view proprietary information stored on "broken" computer hardware while it is being repaired.

Disposal of removable media. You should make users aware that sensitive information stored on floppy disks and other removable media can be recovered even after the files have been deleted. You may want to require users to dispose of all removable media by returning the media to your IT department, where it can be bulk-erased and/or physically destroyed.

Software security. You will need to discuss who has access to application software and its associated data, software licensing issues, computer virus prevention, and software updates and version control.

- **Access control for applications and data.** Application software residing on servers may be accessible to anyone on the network, so you may need to establish specific access control requirements for these programs. Similarly, the data files used by these applications will need to be protected from unauthorized access by users not running the application.
- **Software license agreements.** You need to ensure that employees understand and adhere to the terms of software manufacturers' license agreements, and to make them aware that all software is protected by copyright.
- **Personal use.** Employees should not be permitted to make copies of company-purchased software for their personal use, as this typically violates software license agreements. You may even want to go so far as to prohibit employees from using any software on your company computers for personal purposes.
- **Installing unauthorized software.** All of your software — commercial, public-domain or shareware — should be installed by appropriate IT staff, and should only be used for its intended purpose.
- **Virus control.** IT staff are typically responsible for installing anti-virus software on corporate computer systems, and for configuring it properly and keeping its virus definition files up-to-date.
- **Change control.** Your IT staff should have a software upgrade policy. When a new software version comes out, it will need to be tested for compatibility and security prior to its being installed on the appropriate computers.

Internet security. In addition to creating new business opportunities, widespread desktop Internet connectivity via e-mail, Web and other services has associated security risks.

- **Uploading and downloading files.** Files downloaded or received as e-mail attachments need to be checked for computer viruses prior to use. You may want stricter controls for downloaded application programs, perhaps requiring them to first be tested on non-networked computers to ensure they won't delete files or otherwise damage the involved machine. You may also want to restrict users from uploading certain types of files, or attaching them to e-mail messages — software applications, proprietary source code or other intellectual property, and unencrypted sensitive corporate information.
- **Access control.** Your networked computers may support anonymous file transfer protocols (FTP) to exchange data and applications. You should caution users to not put sensitive internal company information into these systems' publicly accessible directories unless doing so has been approved by management. And you may want to establish a policy of removing all public information from these directories on a regular basis, to minimize the possibility of inappropriate information transfer. Stricter access control via username/password, and possibly authentication devices, may be appropriate.
- **Encryption.** Users may attach sensitive information to e-mail messages, enter it into Web page forms, or upload it to remote servers via FTP. In each of these cases, it is a good idea to require encrypting the information appropriately to prevent it from being intercepted. Your policy should discuss appropriate encryption methods and guidelines, such as using Secure Sockets Layer (SSL) protocols and digital certificates from an approved certificate authority.

- **Privacy.** All users should be aware that their electronic communications may be viewed by third parties; users should either encrypt sensitive company information, or just not send it via e-mail.
- **Personal Internet use.** Typically, users are expected to use the company's infrastructure to access or exchange information only for appropriate business reasons. If you want to allow employees to access Internet services for personal purposes, you will need to define personal Internet usage guidelines. For example, employees may be allowed to surf the Web or send personal e-mail messages from their desktops on their own time, as long as doing so doesn't disrupt other company business; but they should generally not be permitted to access "inappropriate" Internet resources (adult Web sites), conduct non-company business activities, or do bulk e-mailings.
- **Public representation**. Ensure that employees understand that public statements they make on behalf of your company — in e-mail, newsgroups, mailing lists, bulletin boards or chat rooms — may need to be cleared ahead of time with management. They should clearly indicate when opinions are their own (not your company's), and they should be cautioned to avoid any libelous statements.

Network security.

- **Routers and firewalls.** All connections from the public Internet to internal company networks should be protected by router/firewall systems which deny services not explicitly permitted. In addition, you may decide to configure the firewall to only permit services which can be offered securely. For example, you may want to permit TCP, DNS, mail and news feeds from specific news servers, but to block all ping queries and non-authenticated Telnet log-ins. Your policy should define who has the responsibility for maintaining and configuring your network's routers and firewalls, and emphasize the need for strict access control for these systems.
- **Internetworking.** When connecting separate company LANs or WANs, you may want to also require the use of firewalls to isolate them and make their information available only to certain employees on a need-to-know basis. Also, any virtual private network (VPN) connections via the insecure public Internet should utilize encryption to insure information privacy and integrity.
- **Standalone networks.** Standalone networks which aren't connected to the public Internet or to other company networks still require appropriate access control and authentication techniques.
- **Modem use.** Generally, modem access to corporate networks should only be via managed modem pools using access control and authentication. Modems should not be connected directly to users' networked computers. Remote users should not gain modem access to the network via computers that are also connected to some other network.

Physical security.

- **Workstations.** You may want to consider methods — cables, locks, bolts — for attaching equipment to desktops to prevent users from removing computer workstations and associated peripherals.
- **Laptops.** As discussed previously, laptops are easily stolen. You may want to require use of a locking cable or an alarm, and to caution users to never leave portable computers unattended.
- **Servers.** In general, workgroup and Web servers should be isolated and made accessible only to system administrators and appropriate IT staff. Depending on the nature of the information stored on the servers, it may be appropriate to locate the server in a locked room or other access-controlled environment.
- **Network infrastructure.** In a similar fashion, routers, firewalls and other infrastructure systems should be isolated and available only to appropriate IT staff.

Auditing and monitoring.

- **Audit trails.** It's a good idea to maintain an audit trail of user activity, both at firewalls and on Web and application servers. Audit trail log files should be examined on a regular basis by security staff to determine if unauthorized activity has taken place; these log files should typically be archived for a year or so.
- **Intrusion detection.** Network monitoring software tools can be used to sound alarms, alerting security staff when suspicious activity occurs.

Security training and awareness. Your security policy should include a general discussion about the importance of your security training program, and should emphasize each employee's responsibility for attending training sessions and increasing their security awareness.

Contingency planning. Like natural disasters, inevitably a security attack will take place and disrupt your normal business operations. It's important to have a plan in place so everyone understands how to recover and resume normal business operations.

- **Backup and recovery.** Mission-critical application software and data files on all computer systems should be backed up regularly, so they can be restored in case of a security disaster or system failure. Backup media should be tested periodically, and the backup data analyzed to be sure that applications and data files can be restored successfully.
- **Off-site storage.** Copies of backup media should be stored off-site, far enough away to minimize the risk of damage from the same natural or man-made disaster. Off-site storage facilities should meet appropriate industry standards and should provide adequate environmental and physical protection for your backup media.

- **Disaster recovery.** It’s wise to establish a disaster recovery plan for all computer systems and applications which you consider critical for doing business. In general, the goal of this plan is to expedite the recovery of lost data and the resumption of business operations, possibly using another computer system or even at another facility. It’s also a good idea to test your disaster plan annually, and modify it appropriately if shortcomings become apparent.
- **Reporting security problems.** Users should notify security staff as soon as possible when an intrusion or other security problem occurs — even if a problem is simply suspected. Users should report the loss or disclosure of information to unauthorized parties, the loss or theft of passwords (or two-factor tokens), and any unusual system behavior, such as missing files, system crashes or misrouted e-mail, which could be caused by a computer virus. Users should be cautioned not to discuss suspected security problems in detail with non-security personnel.
- **Contacts and information.** It’s important to define whom employees should contact when they have security-related questions, to report security problems, or to obtain a copy of your security policy or related documentation. It may be appropriate for you to develop a security FAQ page on your corporate Intranet, containing responses to employee’s typical security-related questions, and a central repository for public security policy documents.

Disciplinary action. You should emphasize that you will take disciplinary action against any employee, contractor, or other user of your computer systems who commits a security violation. This disciplinary action may include termination of their employment or contract, and those involved may also be subject to criminal prosecution.

IMPLEMENT THE SECURITY POLICY

Communicate the policy

Once you have written the security policy, you need to put it in place within your organization. To do so successfully, you will need to ensure that all employees, contractors and other personnel who access your computer network not only understand the policy, but also why it is required. Basically, you will have an ongoing need to sell your policy to the various constituencies within your enterprise — both upper management and staff — through meetings, presentations, security briefing documents, e-mail messages, posters, newsletter articles and whatever other communication tools you can think of that are appropriate for your corporate culture.

As with any good marketing communication program, you need to articulate the benefits of your product. In this case, your "product" is security. Typical benefits include minimizing financial loss, maintaining a positive public image, helping prevent litigation, and retaining your intellectual property and competitive advantage, as well as just plain keeping the company viable so everyone has a job. In addition to making everyone aware of the big picture, of course, you will need to ensure that people are adequately informed about all the details of your security policy — like how to choose a good password, when to change it, what to do if you detect a computer virus, rules for personal Internet access, and what to do when your laptop computer is stolen. You will need to fully brief new employees on your computer security policy at the time they hire in.

Also keep in mind that your security policy will evolve and change. It will pay to devise standard ways of communicating these policy changes to your organization, like regular security briefing meetings, company newsletter articles or written security policy updates. An underlying objective of all of this recurring communication is awareness — making sure that everyone is thinking about computer security and understands its role in keeping your business healthy and successful. Additionally, it becomes easier to identify personal responsibilities which in turn usually enforcing the policy easier.

Enforce the policy

Administering your security policy may require allocating additional human resources. Your IT or security staff will likely have new responsibilities for access control and authentication. They will need to manage user accounts, passwords, group membership, two-factor authentication devices and digital certificates. In addition, they will likely need to install and use network security tools to watch for suspicious activity. These tools will help them proactively test and verify servers, firewalls and routers to identify security holes or breaches. Similarly, they will probably need to select, install and use watchdog software that monitors network traffic and/or OS commands and triggers an alarm if an event occurs which is contrary to your security policy. In addition, the security staff will need to spend time analyzing log files from Web and application servers, as well as checking audit trails when suspicious events occur. These tasks will typically be in addition to more mundane responsibilities, like backup and recovery, installing new software and updates, keeping everyone's virus definitions up to date, repairing hardware, and assisting employees with their computer-related problems. You should also periodically test the enforcement mechanisms to verify they're providing the intended levels of protection.

When violations of your security policy occur, it will be important for you to take appropriate and consistent disciplinary action. For employees, penalties may range from loss of pay or privileges to firing, depending on the severity and number of the violations. Malicious network access or other violations by outsiders should almost always be reported to the appropriate authorities for possible criminal prosecution.

Reassess the policy

The reality is that once you've written the security policy and have begun implementation, it's probably time to reevaluate the policy. The rapid pace of technology and the astronomical growth of Internet use mean that new security threats appear more and more frequently. In addition to the new security threats, your organization's business strategy may shift. A new business focus can affect your security policy by altering your analysis of the business risks and return on investment evaluations. These factors combine to make it mandatory for you to continually reevaluate and update your written security policy — at least quarterly, if not monthly.

SUMMARY

A security policy is a formal statement of the rules that employees and others must follow when using your company's computer systems and networks. Its purpose is to make everyone aware of their responsibilities for protecting your organization's information assets, and it should specify the details of how to do so. Developing the security policy involves assessing your information assets, security threats, and business risks; putting appropriate policies into written form; implementing those policies; and then repeating that cycle — updating your written security policy on a regular basis and ensuring that everyone in your organization remains mindful of their information security obligations.

It is our hope that this guide has both convinced you that you need a security policy, and provided some insight into the policy-development process. As your security policy evolves, at some point you may decide that you require some expert outside assistance. If so, RSA Security's worldwide services organization offers complete consulting, design, implementation, training and support services.

POLICY EXAMPLES

Following are a few excerpts from various organizations' security policies:

Access control...

"Security procedures must be implemented to prevent unauthorized access to computers, network resources and data. Only employees of [Company] and contractors who have been briefed on the acceptable use policy of [Company] will be given access to the network. Managers shall decide the level of access for each employee. Final permission to access the network will be the responsibility of the Security Committee. Individuals will be issued a unique username. When an employee terminates employment, Personnel will notify the Security Committee and IT, and steps will be taken to disable that user's accounts and access to internal and external networks. Account logon and logoff information will be recorded for security audits."

Warning notice...

"The following notice will be displayed to all users when they access [Company] computer systems: 'Warning: Only [Company] authorized users only are allowed to use this system. Access by anyone else is unauthorized and prohibited by law. Monitoring for purposes of administration and security may take place, to which you consent by proceeding.'"

Password management...

"Passwords will have a minimum of six alphanumeric characters. No common words or phrases are acceptable. Passwords should be difficult for others to guess. Administrators will test for weak passwords. Passwords must be kept private. Do not share them or write them down. Passwords must be changed every 90 days. After three failed logon attempts, account access will not be permitted, and automatic notification will be sent to the system administrator. Highly sensitive systems will generate an alarm after excessive violations. Sessions will be suspended after twenty minutes of inactivity."

Strong authentication...

"Approved products will be used to gain remote access to the network, as well as to highly sensitive systems. Keep strong authentication devices safe. Do not store them with the computer to which they enable access. Report it immediately to the Security Committee if an authentication device is lost or stolen, and administrators will disable the device. The device's associated Personal Identification Number (PIN) or password must be kept private. Do not share it or write it down."

Digital signatures and certificates...

"Only use Digital Certificates from [Company] approved Certificate Authorities. Use digital certificates to identify both the user and the server, and in conjunction with SSL. Protect stored certificates and keys with strong authentication."

Data encryption for data at rest and in transit...

“Encryption must be used to secure data stored in non-secure locations or transmitted over open networks, including the Internet. Encryption must be used to secure at all times any data classified ‘highly sensitive.’ [Company] approved encryption services and products must be used, with a minimum key length of 128-bits recommended for highly sensitive data. Note — the use of any algorithm or device must also comply with the laws of the country in which that data encryption will be used, and may necessitate a shorter key length.”

Encryption keys...

“The keys to be used for encryption must be generated by means that are not easily reproducible by outside parties. Only [Company] approved hardware or software random number generators will be used, to ensure security and interoperability. Encryption keys will be treated as highly sensitive data with restricted access. Encryption keys that must be transmitted, as in symmetrical or secret key systems, must be transmitted by secure means: use of public key-exchange algorithms, double-wrapped internal mail, double-wrapped courier mail. Encryption keys must be changed at the same frequency as the passwords used to access information. All encryption keys must be made available to management via [Company] approved key recovery implementations.”

Public keys...

“In public-private key systems, public keys must be distributed or stored so that they are accessible to all users. Digital certificates may be used to distribute public keys via Certificate Authorities. In public-private key systems, private keys will be kept private by users, subject to the same rules as user passwords.”

ABOUT RSA SECURITY INC.

RSA Security Inc., The Most Trusted Name in e-Security™, helps organizations build secure, trusted foundations for e-business through its RSA SecurID® two-factor authentication, RSA BSAFE® encryption and RSA Keon® digital certificate management systems. With more than a half billion RSA BSAFE-enabled applications in use worldwide, more than six million RSA SecurID users and almost 20 years of industry experience, RSA Security has the proven leadership and innovative technology to address the changing security needs of e-business and bring trust to the new, online economy. RSA Security can be reached at www.rsasecurity.com.

RSA Keon®

RSA Keon is a family of public key infrastructure (PKI) products for managing digital certificates that ensure authenticated, private and legally binding electronic communications and transactions. RSA Keon allows organizations to embrace powerful new e-business approaches with confidence, providing a common foundation for secure distributed systems such as Web e-commerce applications, authenticated and private e-mail, virtual private networks and ERP applications. Modular, flexible and interoperable with other standards-based PKI products, RSA Keon offers more value in a PKI solution than ever before possible.

RSA SecurID®

RSA SecurID is a solution to provide centrally managed, strong, two-factor user authentication services for enterprise networks, operating systems, e-commerce Web sites and other IT infrastructure, ensuring that only authorized users access data, applications and communications. Supporting a range of authentication devices, including hardware tokens, key fobs, smart cards and software tokens, RSA SecurID solutions create a virtually impenetrable barrier against unauthorized access, protecting network and data resources from potentially devastating accidental or malicious intrusion. RSA SecurID user authentication products offer enhanced security to PKI installations, and to the secure applications hosted on the PKI system.

RSA BSAFE®

RSA BSAFE is a family of platform-independent crypto-security development tools that enable corporate and commercial software developers to reliably incorporate security into a wide variety of applications. Today RSA BSAFE technology protects virtually all private Internet communications and transactions, and is the foundation of S/MIME, the standard for secure electronic mail. RSA BSAFE encryption software is also used to secure wireless communications, cable television and data services, and more.

Worldwide Service and Support

RSA Security offers a full complement of world-class service and support offerings to ensure the success of each customer's project or deployment through a range of ongoing customer support and professional services including security assessments, project consulting, implementation, education and training, and developer support. RSA Professional Services consultants have years of hands-on experience helping customers define and implement security policies, including:

- Corporate security policy definition and systematic review planning.
- IT security policy covering system hardening guidelines, password rules, session timeout parameters, and DMZ system administration.
- Public Key Infrastructure (PKI) policy covering minimum key lengths, key expiry, certificate revocation frequency, registration and authentication requirements, key backup and recovery, and trusted signer certificate distribution.
- Service Provider's agreement review for denial of service and security attack provisions.
- Comprehensive logging strategy definition including generating alerts for outages and suspected security incidents.
- Disaster recovery planning and testing.

Contact RSA Security's Professional Services Group if your organization needs help with your specific security policy issues.

NOTES

Corporate Headquarters:
20 Crosby Drive, Bedford, MA 01730 USA
Tel 877 RSA 4900 or 781 301 5000, Fax 781 301 5170

OEM and Developer Solutions Group:
California, USA, Tel 800 PUBLIKEY or 650 295 7600, Fax 650 295 7700

Europe, Middle East and Africa Headquarters:
United Kingdom, Tel +44 118 936 2600, Fax +44 118 936 2700

Asia/Pacific Headquarters:
Singapore, Tel +65 733 5400, Fax +65 733 2400
Japan, Tel +81 3 3539 7511, Fax +81 3 3539 7514

www.rsasecurity.com   info@rsasecurity.com

ACE/Server, SecurID, BSAFE and Keon are registered trademarks, and RSA is a trademark of RSA Security Inc. All other trademarks are the property of their respective owners.
©2000 RSA Security Inc. All rights reserved.