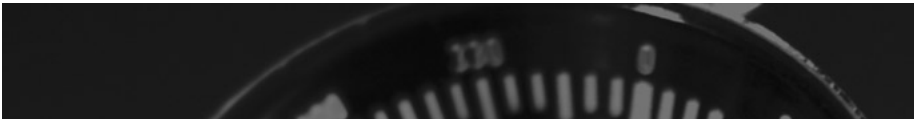
by Eliot Solomon
and The Open Group
Security Forum

guide

Manager's Guide to Information Security

- What to look for when you buy
- Informal and direct
- Addresses key issues for readers who are not technologists

THE Open GROUP



Manager's Guide to
Information Security

What to look for when you buy

By Elliot Soloman
and The Open Group Security Forum

THE Open GROUP

Manager's Guide to Information Security

ISBN: 1-931624-06-02
Document No.: G250 (2nd Printing)

Published by The Open Group, July 2002.

Any comments relating to the material contained in this document may be submitted to:

The Open Group
44 Montgomery St. #960
San Francisco, CA 94104

or by Electronic Mail to:

ogpubs@opengroup.org

contents

Members of The Open Group have asked that we find a way to make the key issues of Information Technology more easily accessible. Some areas, like information security, are vital to the conduct of business, but seem impenetrable to business decision makers. To help address this problem, The Open Group is preparing a series of guides to key issues in information technology.

This Guide

We kept this guide short so that it can be read quickly. It is informal and direct, identifying and addressing key issues for readers who are not technologists. In this guide we do not offer specific solutions, other than what is good practice in any management process.

The small size of this guide limits how much information we can include. We tried to stick to what our readers most need to know, but some of the choices were difficult. Watch for additional guides from The Open Group that will extend your understanding and provide more detailed advice about information system solutions.

About The Open Group

The Open Group, a vendor-neutral and technology-neutral consortium, has a vision of Boundaryless Information Flow achieved through global interoperability in a secure, reliable and timely manner.

The Open Group's mission is to drive the creation of Boundaryless Information Flow by:

- working with customers to capture, understand and address current and emerging requirements, establish policies, and share best practices;

- working with suppliers, consortia and standards bodies to develop consensus and facilitate interoperability, to evolve and integrate open specifications and open source technologies;

- offering a comprehensive set of services to enhance the operational efficiency of consortia; and

- developing and operating the industry's premier certification service and encouraging procurement of certified products.

In the global eCommerce world of today, no single economic entity can achieve independence while still ensuring interoperability. The assurance that products will interoperate with each other across differing systems and platforms is essential to the success of eCommerce and business workflow. The Open Group, with its proven certification programs, is the international guarantor of interoperability in the new century.

The Open Group provides opportunities to exchange information and shape the future of IT. The Open Group's members include some of the largest and most influential organizations in the world. The flexible structure of The Open Group's membership allows for almost any organization, no matter what their size, to join and have a voice in shaping the future of the IT world.

More information is available on The Open Group web site at www.opengroup.org.

The Open Group has over 15 years' experience in developing and operating certification programs and has extensive experience developing and facilitating industry adoption of test suites used to validate conformance to an open standard or specification.

The Open Group publishes a wide range of technical documentation, the main part of which is focused on development of Technical and Product Standards and Guides,

but which also includes white papers, technical studies, and business titles. Full details and a catalog are available on The Open Group web site at www.opengroup.org/pubs.

Trademarks

UNIX is a registered trademark, and The Open Group and Boundaryless Information Flow are trademarks of The Open Group in the US and other countries.

Acknowledgements

The Open Group gratefully acknowledges the contributions to this guide from:

Apple Computer:..... Wanda Cox

Atomic Tangerine:..... Steve Whitlock

California Institute of Technology: ..... Steve Jenkins
..... Vance Heron

Conclusive Logic: ..... Steve Mathews

Hewlett Packard Company: ..... Mike Jerbic

Intel Corporation:..... Carl Ellison

SAP: ..... Regine Brehm
..... Sachar Paulus

The Open Group: ..... Ian Lloyd
..... Ian Dobson

Tivoli (IBM):..... Bob Blakley

Chapter 1
Audience and Authors

Is this for you?

Information security is a critical part of doing business today. If you're a manager, it's very likely that you have to deal with information security issues from time to time. If you haven't been trained to deal with security issues, and if security hasn't been clearly explained to you, this guide will help you to do the security part of your job. If you already understand the issues, it will help you communicate them to your colleagues.

If you need …

You should read this guide if:

- You are a business manager responsible for some aspect of your organization's information technology systems.
- You need to evaluate or approve information security purchases or expenditures.
- You don't yet feel confident discussing information security with vendors and technologists.

What we can offer

Reading this guide won't make you a security expert (we don't think it would be a good use of your time to become an expert), but it will help you talk to security experts and make informed and confident decisions about security.

Who we are

This guide was written by the members of The Open Group Security Forum. This Forum has existed for more than 10 years and brings together security professionals with a wide range of experience from a wide variety of organizations. As part of The Open Group, the Security Forum works to develop software that meet the needs of real businesses, and the standards that ensure that you can buy products from many suppliers with the assurance they will work together.

The members of the Forum represent both producers and consumers of technology. Some are technologists and others are policy makers. Their organizations are headquartered all over the world, and represent a broad cross section of businesses from Europe, Asia, Australasia, and North America.

Many of the information technology industry's leading security experts participate in the Forum on a regular basis, and the Forum invites outside experts to every meeting in order to keep abreast of important developments in information security. The participants have a valuable perspective on information security in a business context and would like to share it with you.

Chapter 2

Why Security Matters to Your Business

Ignore the movies

Popular fiction is not reality. Hackers, crackers, spies, and government agencies running amok are not what security is about. And it's not just about the Internet. As a business manager, you should treat data security as an ordinary part of your business. As you read this guide, you will learn that good security solutions help you address the routine needs of a business that is run accurately, with reasonable levels of control and accountability for the activities of employees, customers, and business partners.

eCommerce is real

Of course, the Internet is now as essential to business as the telephone, and a lot more powerful. We're not talking about "dot coms." We're talking about businesses like yours that use the Internet to make it easier for their customers and suppliers to do business with them. Good security solutions will help you do that business. Reliably. Safely. Easily. If a security solution makes it harder to do business, it's not the right one for you.

Improve your business

Some people think eCommerce is only for startups and "tech" companies. In fact, eCommerce systems give every business, big or small, a set of tools to do business better.

It would be an odd business that had no suppliers or partners. If you have suppliers, subcontractors, or vendors; if you buy or sell materials or subassemblies; if you work with others for marketing, design, advertising, or distribution; if your business isn't an island to itself, you can probably use the Internet to improve your business processes. Hot words here are "collaboration," "supply chain management (SCM)," and "virtual marketplaces." But how does this affect you?

Like many, you may be finding that your customers are ever more price conscious and demanding about quality and service. For this, you have to be even more efficient, and effective.

Partner effectively

You have to manage your inventories, receive and deliver products just in time, generally be more efficient, and always know where you stand. You want to get your suppliers and partners to help. This is sometimes called Supply Chain Management. From your perspective, it's just good business, done even better.

Collaboration goes beyond managing deliveries to and from inventory. All sorts of systems and processes in your company may be linked with those of your partners. We've mentioned engineering and design, sales and marketing, and a number of other obvious opportunities to work with partners over the Internet. Almost anything you do inside your company using paperwork processes can be shared with partners outside your company over the Internet. How far you might take it is limited only by your creativity as a business manager and entrepreneur.

Engage your customers

Your customers are becoming more demanding. After all, customers can buy whatever they like, whenever and wherever they like. Companies need innovative ways to create and exploit opportunities to give value to their customers. Don't stop with a simple web site that just takes orders. You must offer your customers something extra to keep them loyal. You need to maintain strong, even intimate relationships with your customers.

Customer Relationship Management (CRM) is the name that's given to this relationship building when it's done using information technology. CRM aims to improve interaction with the customer in all phases of the relationship cycle. It's more than just keeping your clients' accounts in order: it's about knowing their needs better than ever before, and helping them take the greatest advantage of what you have to offer.

Governments and regulations

The Internet is also changing your company's relationships with governments and regulators. Enlightened government agencies are doing the same things enlightened businesses are doing: they're making it easier to do business with them through the Internet. Like many influential private companies, some governments now strongly encourage the use of eCommerce techniques by those who need to do business with them.

For many businesses, governments have a more direct influence on security choices. You may be subject to regulations that require you to protect or control certain information. Increasingly, laws and regulations are requiring businesses to ensure privacy for client information. Your choice of ways to meet these requirements may be controlled in whole or part by regulation. In some cases, the use of (or failure to use) specific techniques may affect the protections you have under the law. And the reach your company gets by using the Internet may subject you to laws and regulations of more than one jurisdiction or country.

In summary …

Opening up your business to closer, more collaborative relations with your trading partners and customers brings us back to the topic of this guide: security. Good security systems will be as sensitive to the need to be open to partners and clients as they are to the need to be closed to strangers. They will be as capable at helping you manage and take advantage of the opportunities of the Internet as they are at guarding you from danger and loss. And remember, running your business in a safe, assured way is as important on the inside as it is from the Internet.

Chapter 3
Security from a Business Perspective

So what should you do now about information security? You should do what you do about anything affecting your business. Decide what you want to accomplish, then look for the best way to build or buy the means to reach the goal. You'll make the usual sorts of trade-offs along the way, then incorporate the solution into the way you do your business. Sounds simple. And complicated. Well, that's business. Doing just the simple things won't get you ahead of your competitors. Only the hard things do that. But failing to do the simple things is still the quickest way to get taken out of the race all together. So you've got to do both. You shouldn't need to be a technology specialist to do this; you should do it in a businesslike way! That's *your* job.

It's your corporate policy

At the center of every corporation is a set of goals and objectives that drive its operations. Many organizations are structured into functional units (such as manufacturing, sales, marketing, finance, operations, and so on) to achieve their goals. Some are organized by lines of business. All organizations are, of course, made up of individuals. Policies keep all the parts of the organization pulling together toward the goals.

Whether they are written out in a corporate manual, or informally shared as "the way we do business," your business policies describe how you work. They tell who can and should do what, and under what conditions. ("Employees may accept gifts from vendors, provided they are not valued at more than $50 and give no appearance of impropriety." "Expense reports should be approved by the immediate supervisor unless he is unavailable, or the expense report exceeds his signing authority.") They also tell your people what they can't or shouldn't do. ("Employees may not take office supplies for their personal use." "The secret formula may not be copied or removed from the manufacturing site.")

You can see that these policies relate closely to what you want security systems to do. A good security solution will help you enforce company policies about use of your information systems, and the information and services they support. A better security solution will help support and enforce policies about how you do your business. A security solution that requires you to change the way you do your business to meet *its* notion of appropriate policies is not one you should use.

We'll talk about policy quite a lot in this guide. We believe the most important thing a security solution does is support the policies that help you run your business safely and well. You have to do your part to make this possible. Make sure you really know your policies, and review them periodically. Business and the competitive environment change, and your policies will change as well. Be sure everyone in your company knows what your *current* policies are. And please, tell the people providing your security solutions that you have policies, that you want them to be included in the design of the security systems, and that you will need to be able to update them easily in the future.

How much security do you need?

How good does your security need to be? That's a business question. It depends in part on how important it is to protect your business, its assets, your clients, and yourself from particular risks.

Some authorities suggest the answer to this question should be based on the "value" of the thing you're protecting. They say you should not spend more to protect something than it would cost to replace it. Some authorities emphasize the eCommerce enabling aspects of security, and recommend you not spend less than it takes to get an advantage over your competitor.

Like every choice a business makes, the choice of security solutions involves many factors that can be objectively measured, and many that are subjective. It involves protecting your balance sheet, your competitive position, and your reputation. And, as you know, businesses rank these concerns in many different ways. How do you choose a security solution? The same way you make any other business choice. Here's our advice about how to begin.

What are the risks?

The words risk and threat are often used as if they were synonyms. They're not. Risk measures the harm your business might sustain. Threats are the things that can cause the harm. Some risks you might face are the loss of

your customer list, or your business being shut down for a day or two, for example. Some threats you might face are attacks by disgruntled employees, erasure of critical files by inexperienced operators, or denial of service attacks from the Internet.

You should focus on identifying and valuing the risks that are significant for your business. Identifying threats to your information systems is a technical task that should be done by trained security specialists, once you tell them the risks you believe are important to your business.

What sort of protection?

It's not likely your company's information systems are involved in National Security. You are probably not the target of espionage by the security services of a powerful nation. And you probably don't need to use the same approach to security that your national intelligence agency uses. Unfortunately, much security technology on the market today is based on military and espionage related security requirements and protection methods. That sort of security system is often a poor match for ordinary businesses. Don't be impressed by a security product that's right for the CIA unless it's also absolutely right for you.

On the other hand, don't get complacent about the risks you face. And don't assume that, because you don't face much risk, security isn't relevant to your organization.

A simple example

Consider an organization whose Information Technology is office automation — a network of PCs used for word processing, preparing invoices, some spreadsheet analysis, and the like. The users share a printer or two, and, maybe, do a bit of file sharing. If it's not connected to the Internet (a big assumption), this office won't need a lot of security, but it will benefit from some elements of a security system. Many "off-the-shelf" software programs, including operating systems and common office suites, assume that there is at least enough "security" to be able to tell one user from another. Why?

Because it lets the software program be more useful to the users, and can help them work more efficiently. It will allow them to add comments and edits to documents they collaborate on; they will be able to customize their work environment and tools to their individual preferences; it will let the system help its users track what they were working on, and find the things they find most useful. It makes it easier to keep track of who's doing what, and which file or printout belongs to whom. That, in turn, can help you address a risk every business faces: the possibility that employees will mistakenly misfile, erase, edit, or otherwise damage their coworkers' work.

That was a very simple example, and we chose it to illustrate a few simple points. Two are: "security enhances the user's experience," and "risks emerge even in small things." And we'd like you to reach two additional conclusions: "convenience and efficiency reduce risk," and "there is no hard separation between security functions and business functions."

Most likely you're using your information systems for more than just office automation. And you've probably connected them to the Internet, if only for the sake of email. So your needs will be more elaborate than those in our office automation example. You may have information that is much more sensitive or you might use your systems to control critical business processes. You might be connected to the Internet; maybe you let employees, customers, or business partners use your systems remotely. However complex your information technology enabled business, remember the basic lessons of the office automation example. They apply to everyone.

Information at risk

Your security solutions must protect your company's own information. They must also protect information that the company has, but which belongs to others, such as your business partners, employees, and clients.

Inadequate security for your own information can put you at risk in a number of ways. How much would you be harmed if a competitor saw it? If it was released in the newspapers? How much would it cost to reconstruct it if it were destroyed; how long might your business stop while you recover and restore the information? You know the questions, and you probably

know many of the answers. They are general business questions, not specifically data security questions. You don't need to understand hacking to understand these risks.

A more difficult problem is determining what the information you have is worth to others. This is particularly important when your systems are holding data that belongs to other people, or in which they have rights. This includes business related information from your business partners, your vendors, and other companies.

More challenging, though, is valuing the information you have about people. You know that Human Resources files are sensitive, and shouldn't be inappropriately disclosed. But have you considered how *your employees* value that information? What is the monetary value *to them* of keeping that information private? How would that compare to the value *you* place on your company's own information? Consider this carefully when you plan your security for employee information.

You have similar issues with information you've collected about your customers. Their credit history, buying habits, demographic information, and similar information might be valuable to them, or, more likely, it might be worth a lot to them not to have that information get out.

More than information

Of course, there is more to protect in your organization than the information in your information systems. Your business processes need protection as well. Only authorized users should be able to enter orders, start the factory, and initiate the payroll process. What processes have you automated? How much control do you have (indeed, should you have) over who gets to control them?

The systems themselves also need to be protected. Your web site should be guarded against defacement. PCs mustn't be taken over by anyone other than the assigned users and the office automation administrators. Database schemes should only be changed by database administrators, and only according to defined change policies. Don't think of security as

protection from "bad guys." You and your security system should focus on making sure your corporate policies are followed: who gets to see or do what, when, and under what circumstances and procedures.

Don't go overboard

Don't overestimate your importance to others. We assume that the day to day internal workings of most businesses are not especially "interesting." That's not to say they don't need security, but you don't protect costume jewelry — no matter how important it is to you — the same way they protect the Crown Jewels. That's because other people won't find it worthwhile to mount a sustained or vigorous attack to steal it. But there are exceptions.

If your company is the target of specific attacks, either rationally or irrationally motivated, the value an attacker may put on getting at even seemingly ordinary stuff may be surprisingly high. And information that is usually innocuous may, in the hands of a motivated enemy, be surprisingly damaging to you or your company. You probably know if you've got those kinds of enemies. If you do, adjust your security requirements appropriately.

IT security as a service

In addition to protecting information and systems, information security should provide services that help run your business more effectively on a day to day basis. When you procure a "security" solution, consider whether it could contribute to the solution of other business problems. And consider whether the solutions you have for those other problems might contribute to your security solution. Here are two examples.

Employee management is important to organizations of any but the smallest size. You probably have someone or some group that keeps track of who are the company's employees, and knows at least something about the employee's function in the company. Payroll, finance, and human resources departments usually have or need a lot of the same information your security system needs. Keeping your security systems "in sync" with

Human Resources is as important as synchronizing your payroll systems. Look for common solutions that reduce cost and improve efficiency.

Audit and controls are critical to the conduct of your business. You probably have some form of record keeping that assists you in controlling your finances and maintaining your audit. These are often corporate functions that provide consistency across all business units and functional areas. Your security services will have similar requirements for record keeping and audit. Try to develop compliance and audit techniques that serve both financial and data security policy needs.

A very good security system will help you with more forms of control than just limiting access to computing systems. It could manage access to physical facilities to certain people at certain hours on certain days. It could allow only selected individuals to perform various business functions, like modifying an inventory database, or transferring money between accounts. It can also be used to ensure that policies requiring multiple levels of approval for specified transactions are followed. Don't miss an opportunity to tie all these things together for your firm.

Responsibility

You'll notice that we haven't yet talked about the role of the "security administrator" in updating all this information. That's because we think that's not necessarily the best thing for your company. We think your security administrator should set up the basic rules for the security system itself, and take care of the technical and operational configurations of the system. Entering business information, like who works for the company and what department or project they are in, should be the responsibility of the same people who handle that information for general administrative reasons.

These actions (business controls) are best done in the context of an *ongoing* and *consistently applied* system of checks and balances with processes and procedures in place that verify those checks and balances. Make sure your security system supports an appropriate set of checks and balances on the control information it is given.

Often, security related decisions are handled at the level of business units or departments. Assignment of staff to particular projects, with the "right" to get to the project's data, is an example of a departmental decision with security consequences. A really good security system will make it easy for these departmental decisions to be entered directly into the security system at the department level. Of course, the security system has to make sure that only authorized personnel make the entries to the security system.

Activity logging

Many information security systems have the ability to log actions that affect data in your information systems. This log information serves several purposes, including helping to determine whether a system has been compromised, what information has changed, and measuring normal and unusual loads on the systems. In addition to supporting investigations into information system compromises, log files usually contain information that can be used to help get systems running again after a problem.

When planning a logging system, consider how much information you need to capture, how long it will be stored, and how it will be monitored so your policies are properly supported. Too often, audit logs are ignored until after a crisis has happened, at which time they're reviewed, only to show that evidence of impending problems had been available days or weeks prior to the crisis.

Detection and response

Remember, a completely secure system is impossible. You must be able to detect and respond to failures in the enforcement of your policies. Information security systems should monitor your systems to identify anomalous patterns of activity. This monitoring, together with the logging and audit functions described above, will also help you (or you auditors) to determine that those responsible for setting up and maintaining the system have done the job correctly.

Awareness and training

People are often the weakest link in securing information. Awareness of the need to protect information, training in the skills needed to use systems securely, and education in security measures and practices are essential for the success of any organization's security program. A good program of awareness, training, and education will improve employee behavior and attitudes towards more than information security. It will cover all aspects of employees' responsibility and accountability to your business policies, and make security an integral part of your everyday practices.

To be effective, your training and communication about information security must be creative and frequently changed, like advertising. It must teach specific security related job skills and reward practices such as protecting the physical area and equipment, protecting passwords, and reporting security violations.

Using what you have

You may ask why, after buying all that information technology, you have to also buy security solutions. When you buy a car, for example, it already comes with locks and keys. Why doesn't information technology also come with its own security? In fact, it often does. You may find that you have already bought portions of your security solution.

Operating systems usually provide password protections and basic user management. Databases often have security services that control access, as do ERP systems and other high value information technology products. Try to take advantage of these to the greatest extent possible. But don't take for granted that those security services will automatically contribute to meeting your overall policy objectives, or that they will do everything you need. Some buyers of automobiles still feel a need to augment or modify the security features that come from the factory, or keep it in a secured garage.

It's possible that the security features of different IT products you have will not work together. Sometimes the security features of a business application are designed only to secure that product; worse, some vendors specifically try to keep their products from working with their competitors' products. Most often, security features don't work together because, today, there is no master plan and few standards for different vendors to use as a guide. The Open Group is one of a number of organizations working to create standards to improve this situation.

Even if the products you buy all work together correctly, they may not "automatically" set themselves up to meet your objectives. In fact, many systems "with security" are delivered with the security turned off. When you choose to rely on the built in security features of the software you've purchased, be sure someone competent has checked the way they are configured.

Chapter 4

What to Expect from Security Solutions

Now that you know how to think about security, let's apply that reasoning. Let's look at the things you should expect from a security product.

Simply, a security system follows your company's policies, and ensures that only the right things happen, and that, if wrong things happen, you are told that they did and, ideally, who did them. What do security products need to do to meet this simple objective?

One thing is the ability to protect information from modification unless and until a modification is authorized. Another is to keep secrets and ensure privacy. Another is to ensure nothing is used, moved, or eliminated without proper authorization. To be able to do these things, a security system should be able to recognize who is and isn't authorized to see, change, or share information, and who has the right to say so. Let's break that down, and see how it's done.

Administration

Ultimately, the purpose of a security system is to make sure that your company policies are followed. For it to do that, there must be a way to supply your company's policies — and the details of how they are to be enforced — to the system. For example, one policy might be "only officers of the company can approve requisitions above $8000." Another might be "only customers with active accounts can place orders through the web site." You'll also need a way to let the system know who the officers or active customers are. Security systems must have administrative services that make it easy to set up policies. Good systems let systems administrators do this. Better systems make it easy for business administrators to set up policies for your security systems.

You have to know what you want your security system to do. It's not magic, so don't expect the impossible, but don't expect too little, either. It's got to do what you need done, or else why buy it? Remember, if you don't set up the system to do what you need, or if you don't take the time to give it *all* the policies you need enforced, it won't be able to do the job. *Security systems don't read minds*.

Assurance and audit

Once you've deployed a security solution, you ought to know that it actually is doing the job. Better, the system should allow you to prove to others — like your insurer, auditors, and directors — that you set it up to do what needs to be done, and that it's doing it correctly. Some businesses may be required by law to prove they are following correct security practices!

A good security system will help ensure that it is only used correctly, and that once it is set up it isn't changed without proper authorization. It should record all changes made in its configuration and the policies it's supplied so that you can always check that things are as they should be. Ideally, it will record who made the changes. (Because even authorized access may result in a security breach, *all* changes should be logged with the identity of the person making the change.)

A better security system will also keep records of the work it does — the things it has allowed to happen, and the things it has prevented — so that you can check not only its work, but also your own. With this type of information you can check whether the policies you created really accomplish your objectives. The best security systems also have mechanisms to monitor what's going on, automatically test the system, and report promptly when things seem to be going wrong.

You may want your security services to go a step beyond this. To assure its own performance and keep track of changes made to it, a security system must keep logs and audit information. Some security systems let you use those audit tools to record and review transactions that pass through them. This can be very valuable information for you — not only to evaluate your security, but also to assure your business. Security systems that do this well are few, and generally very expensive. It won't always be that way, so it's something you might consider.

Protection

Mainly, what you administer and assure in a security system is its ability to protect things. Protection is one of the most fundamental things a security system does. It keeps things from being seen, used, changed, or

discarded inappropriately. Security systems protect things by separating protected things from everything else, and placing a guard between them. For example, to protect your company's network from the rest of the world, you might use a firewall as a guard. To protect your email from the prying eyes of your subordinates, you might use an email program with a password protection system. To protect your data center from unauthorized visitors you might use a badge reading system.

Different security systems are designed to protect different sets of things, using appropriate forms of guards. No one system will protect everything; you have to make sure that you get the right set of guards to meet your protection needs.

No matter how good your security system is, it *can* be compromised, with enough time or effort. A good security system will give warning that it is under attack, so you can call in the cavalry. A very good security system will provide the evidence that will help bring the attacker to justice. But you *must* be prepared to step in to assist when the system calls for help.

Know who's who

Your security system should be able to recognize people (or companies, or the computers used by people or companies) so that you do business only with the right people.

We already discussed the advantages of linking your security system's list of employees with the list maintained by your Human Resources department. That's a good thing to do, but may not be practical in all cases. Even if you don't link the systems, remember that your corporate policies and practices link them. For example, how do you check that a candidate is who he claims to be before you hire him? Maybe you don't. Maybe you ask to see a birth certificate or a school transcript. Maybe you hire an investigator to do a background check. It's a business policy choice. Your security systems need to support those same sorts of policies. You can't rely on your systems to "know" somebody if you don't enroll people with care. And, of course, what's true for employees is also true for customers, suppliers, and business partners. You may need a security solution that keeps track not only of who you know, but how you know them.

Proving "who"

Knowing who the employees (or customers) are (and why you believe them) is the first step. The next is to "recognize" them when they try to use your systems. This includes, for example, employees logging onto PCs in the office, potential customers using your web site, and trading partners sending messages representing orders or invoices.

Systems that "prove" who a person is are sometimes called authentication systems. Some are simple, like a bit of a program that checks a password. Some are elaborate, like systems that recognize fingerprints or voice. Remember, none of these systems are foolproof. None! Errors can be made, like mistaking one person for another or failing to recognize someone who should be known. Some systems are more prone to abuse than others. Have you ever let someone use your password, for example? How did you take it back? If a system requires some physical "token," the token can still be shared — which may still be a problem — but it can be retrieved. There are always trade-offs: reliability *versus* cost, convenience for the user *versus* certainty for the auditor.

Managing the list

Keeping track of the people — and of the sort of evidence that can prove they really are who they say they are — can be a big problem. The problem becomes more difficult as the number of people you need to identify increases. It becomes still more challenging if you require more rigorous proof of identity, or if you need to support more forms of proof (password and/or badge and/or fingerprint and/or smart card). Tracking this information for your own employees will be hard enough. But suppose you need to recognize the employees of your business partners.

This function is often served by a system called a registry or a directory. (You may hear about something called LDAP. It's one kind of directory that can be used for this purpose. Active Directory™ is Microsoft's version of a directory service. There are others as well.) Sometimes the registry is built right into a security system. For example, some web servers keep their own lists of users in their security subsystem. If your "people management" and security requirements are not very complex, security systems with built-in

registries may be appropriate. If you need to coordinate the activity of a lot of security (or secured) systems, or you need to specify sophisticated security policies, a separate registry or directory that can be shared by many systems is probably a better approach.

What to allow

Services that "decide" whether something ought to be allowed or not are authorization services. Some security vendors will suggest that all you need to make an authorization decision is the identity of the requestor. In some cases that's true, but sometimes it's not. Often there are more things to consider. For example, your policy might be to allow certain things to be done only during (or after) business hours. You might care more that a request comes from inside a trading partner's organization than you do who the individual is. You might want to base a decision on prior experience with the same person. And so on.

As with the identity services we discussed above, authorization is often built into systems, along with management of the names and identities of the authorized users. It can also be handled by a separate authorization service. As with identity services, the more complex your authorization policies, and the more systems you need to coordinate around your policies, the more you should consider a separate authorization service.

Secrecy and privacy

Secrecy and privacy are similar, but not exactly the same. In the last few years, laws and regulations have created specific "privacy" obligations for many businesses, making it more important to understand the differences between these functions. Secrecy is protecting *your* secrets from disclosure. (Protecting them from being destroyed is something else.) "Privacy" is keeping your organization from disclosing *other people's* information without their consent.

We like to think of the right to privacy as being the right to be left alone, not to have anyone intrude on you. A good security system should help your company ensure that the information you have about others doesn't

leak out. A better security system will help you ensure that no one in your organization inappropriately gathers or uses private information — that you don't violate anyone's privacy. Information that needs "privacy protection" includes employees' personal information and customers' account information. Even information about what services a client uses may be sensitive, private information.

One thing to keep in mind is that your security system only protects things inside the guarded perimeter. It can't protect things on the outside. And it can't protect things on the inside if they are "sent" outside. Once you have shared information with others outside the control of your security system, you will have to trust them to keep the information secret or private. So called copy protection mechanisms and other "rights management" technologies will not protect your information from inappropriate use. They *may* help you identify who violated your trust. Even then, your avenues of recourse will be probably limited to what you have arranged by contract or the protections of civil law.

Build confidence

So far we've discussed how security systems protect things from misuse. Security systems can also help protect people from being deceived! They can, to a certain extent, help you know who and what to trust, and they can help you earn the trust of others.

The first way security systems let you tell what's true is by giving you confidence in the operation of your own business. You are probably more comfortable relying on documents filed in an organized system under lock and key than you are on documents that are stashed here and there, with no one in charge of them. The same goes for information in your IT systems. To rely on the accuracy of the information in the systems, you have to have good policies for access to and modification of the information, and the policies must be reliably enforced.

Once you are confident in your own business practices, the next step is to allow your customers and partners to share that confidence. This is often done using cryptography — the science of secret or hidden writing. Cryptography is used to keep secret information from being seen by the wrong people. In IT security it is also used to create "digital signatures" that let you know with whom you are communicating.

Confidence in documents

Security systems can also give you more confidence in specific pieces of information, whether they originate in your business or on the outside. One way is by providing "digital signatures" for important documents. Things that are commonly signed in the "real world" may need also to be "signed" in IT systems. Some of these are mail, contracts, purchase orders, and expense reports. Digital signatures are like "real" signatures in many ways. A digital signature is a "mark" that is recognizably that of a particular signer, and *relatively* difficult to forge. A "real" signature relies on an individual's handwriting to make it distinctive; a digital signature relies on cryptography. Neither kind of signature is forge proof. Both kinds of signature can be "guaranteed" or "notarized" to make it easier to prove that the signature is genuine. But just like "real" signatures, whether a digital signature will stand up in court depends on the laws of evidence in use, and the power of the evidence presented to support or refute a claim of forgery.

Digital signatures have a curious property that "real" signatures don't. A "real" signature is placed *on* the document it goes with. It can't be separated from the document without leaving a mark or a tear. A digital signature *contains* a "fingerprint" of the document! While it can be physically separated from the document, it is always possible to tell which document a signature was attached to. Because of this odd property, a digital signature can help prove that a document hasn't been changed since it was signed. If the document is changed, the fingerprint inside the signature will reveal the fact! So digital signatures are, in some ways, more powerful than "real" signatures.

But, as we said above, signing a document doesn't automatically prove that either the signature or the document is authentic. Reliable proof depends on evidence, and more complete evidence costs more to create. If you decide to

use digital signatures, your signature system should create an appropriately complete record of the signing transaction for your customary business practices. It should be able to be more rigorous when necessary. (The same goes for checking evidence when you receive a signed document: check as much as you customarily need to, and more only when appropriate.)

If you rarely need more detailed analysis, you may find that the best solution is one that does detailed checking in a cumbersome and expensive manner, but is extremely efficient for your normal case. If you often need to do detailed verification of signatures, you may want to buy a system whose basic operation is more burdensome, but doesn't take such a cost "hit" when you do detailed verification.

Keeping trust

Cryptography is a powerful tool for proving who you are, and for protecting information. But since it is based on "secret writing," it's of no use if you don't have a reliable way to share secrets. Think of a "secret password" you might give to enter a private club. To be any good, all club members must be given the password, but it must not be given to anyone else. Remember when Chico told Groucho, "You can't come in here unless you say 'swordfish'." (From the Marx Brothers' movie "Horsefeathers.") Because he gave the password to a nonmember, Chico broke the trust club members had that only other members would be admitted. If you want to use cryptography, how do you safely share the secret password and maintain the trust of others who rely on the secret?

There are a variety of ways to do this available today. One technique is called Public Key Infrastructure or PKI. There are products from a number of vendors that use PKI. (Some people say "PKI" when they mean products that use PKI to enable cryptography or digital signature.) Another product that shares secrets is Pretty Good Privacy or PGP. (The PGP product is really a cryptography and digital signature service that includes its own secret sharing method.) Yet another mechanism for sharing secrets is the Kerberos system, which was invented at MIT. Probably the best recognized system that uses Kerberos is Microsoft's Passport. "Which system is best for you?" is a question you have to decide, almost certainly using advice from your technical experts.

Extend your reach

Security systems protect by placing "guards" between a protected space and the rest of the world; the "outside." This model is often used by companies that put firewalls in place to protect the "inside" of the company from the "outside" of the Internet. Sometimes this inside/outside arrangement is too limiting, as when a company has employees who work from home, or travel on business. Even employees who, while in the office, use any of a variety of mobile communications technologies have this inside/outside character.

Sometimes you might want to treat someone in a different firm, such as the purchasing officer at one of your clients, as if he were "inside" your firm. There are a number of ways to extend the "insideness" of your company's systems to people on the outside. One of these is the Virtual Private Network or VPN.

The key word here is "Virtual." The VPN is not a physical network; it is a protected channel created by its owner through someone else's network, or through a public network like the Internet. It protects communications from being intercepted or changed while in transit. (A VPN by itself does not tell much about who is at "the other end.")

A VPN can provide a route from the outside to the inside that is secure but temporary. It is created when and where it is needed, and it disappears when the communication process is complete. When a properly operating VPN is finished it leaves nothing behind that could compromise security.

Smell trouble

Content scanning is a tool most often used in conjunction with email. The software will examine each mail item being sent outside the organization and look for specific words. The choice of words or phrases depends on the company's business, so the software is configurable to allow it to scan for any word or phrase. (Content scanning can also be used to check incoming email for offensive or inappropriate content.) This process takes time and computing power, so, if you need content scanning, be sure to budget for it explicitly when you plan your security systems.

How important is content scanning? For most businesses that's a subjective judgment. But in some industry sectors, it is a duty for the company to scan communications. In the finance industry in particular, companies must take precautions to stop money laundering activities, fraud, and theft. Content scanning can help detect this.

This approach may oblige you to keep accurate records to establish the origin of any inappropriate content. You will probably be required to have an email policy known to all employees that informs them that their mail may be scanned. This can help you avoid liability and litigation by your employees if scanning finds something untoward and you apply sanctions against the employee involved.

Of course, content scanning is only as good as the selection of words you make. If you use content scanning, make sure you monitor how well it supports your policy objectives, and adjust it as necessary. Don't just use content scanning to block the offending messages. Capture the results of the scanning, and combine it with other information from your security system and other systems. Careful attention to patterns of policy violation can help you identify and head off future problems.

Another form of content scanning is virus detection. Services of this sort scan email, files, and other parts of computer systems to identify and, sometimes, eliminate the bits of malicious software program that can attack computers and their contents. Viruses can be introduced in many ways, not just through email, so virus scanners are usually deployed differently compared to the content scanners we described above. Computer viruses, like the viruses that cause diseases, are sometimes detectable only by the symptoms they produce, so virus scanners do more than scan for viral content — they also look for the effects viruses have on your systems.

Detect problems

As we said, even the best security system can be defeated, given enough time and effort. Good systems include the ability to detect signs that the system's protections are being breached. One part of this is intrusion detection. Intrusion detection is a combination of hardware and software that detects attempts to penetrate your systems, and searches for the signs that systems have already been tampered with. Despite their name, good

intrusion detection systems don't just detect intrusions. They will also detect unauthorized or inappropriate use of systems by insiders; incorrect installation of software packages; operator and administrator errors; anything that will tend to degrade security.

Problem detection is hard, because it includes so many things. Remember that, like all aspects of security, intrusion detection can never be perfect. Your goal is for it to be sufficient for your needs, and as effective as possible at the most reasonable cost. To achieve this, all the parts of your security solution must work together. The more "hints" the protective and administrative systems give the intrusion detection system, the easier it will be to get the evidence of problems. The more intrusion detection integrates with audit and assurance, policy management, and so on, the easier it will be to analyze the evidence. Security systems must work as a whole.

Work as a whole

An important thing you should expect from security solutions you buy for your company is that they will work correctly together, regardless of who you bought them from.

There are two main ways to achieve this. If you can select products that are designed to work together, you'll be in good shape. But it's unlikely you'll find many products that do this, so you'll probably need to buy more products that tie together all the others. That can add complexity and cost, but is often the best the vendors have to offer at the moment. The situation will improve with the development of standard approaches to security solutions, and technical standards that will help vendors build and buyers recognize products that *will* work together.

But sometimes the best way to get your solution to work as a whole *is* to use products that link other elements together. Some security solutions are improved by using fundamental services to link and harmonize their parts. Authorization and directory services are expressly designed to tie security solutions together. Administration and audit systems can also help coordinate the parts of a security solution. Over time, solution providers will develop systems that will coordinate security systems by automating the process of creating and managing policy.

What exactly does it mean to "work as a whole"? From the perspective of your company's requirements, working as a whole means your policies are consistently understood and applied across all your security systems, and the business systems they protect. Things that help achieve this include centralized administration, a common policy base, and tools and user support that make it easier to get it right than to get it wrong.

From the user's perspective, working as a whole means that getting into the systems he needs will be straightforward and easy. "Single sign-on" is an example of making it easy for the user: once he's logged on to some system, all other systems will recognize him automatically. Next best would be if the user didn't have to remember many different passwords. (Actually, for many organizations "reduced sign-on" is best. The user has one password for routine functions, but special passwords for special functions.) And with one or many passwords, if the user doesn't have a clear understanding of his rights and privileges from one system to another, it will be difficult for him to use the system correctly and properly understand and comply with your policies.

There are security solutions that try to do this for the user. But beware: some make it easy for the user to get into different systems by "punching holes" through those systems' own security solutions. (Unfortunately, how to tell whether they do is beyond what we can explain in this guide.)

What it can't do

But remember, just buying security products or services and installing them in your business won't eliminate all security problems. There are some things a security solution will never be able to do.

It can't protect you from misplaced trust. Once you've trusted someone with important responsibilities, your security system won't second guess your decision. If the person proves untrustworthy your security system won't be able to protect you from him.

It can't reverse time's arrow. If you've already suffered a loss, or made a policy decision that worked out badly, no security system can undo the harm.

It doesn't provide "insurance." Good security is *not* insurance. Insurance covers the risks left over after you've done your best to protect yourself. Security systems are like fire suppression equipment, not casualty insurance.

It can't protect you from yourself. *You* have to follow "best practices." *You* have to review your policies and practices on a regular basis to make sure they still meet your business objectives. And *you* have to stay on top of how things have changed, in your business and in the world around you. But that's your job as a business leader! It's not something new that grew out of the Internet. As a business executive you must stay engaged with IT security professionals in the same way you stay engaged with your financial advisers and market analysts. If the goal really is to run your business well, it won't do for you to delegate security policy to techies.

Chapter 5
What to do Next

We hope this guide has given you the information you need to begin assembling a security solution for your company. Now you need to decide what to do next.

Most firms will choose to use their own staff to handle some part of their security solutions. Some will try to do it all on their own. We suggest that there are very few firms that can do it all on their own, and not many that can leave it all to outsiders. The realistic choice is to decide how much you can reasonably do for yourself, and then to find others who can do the rest for you.

Doing for yourself

The first things you should consider doing on your own are the things that are routine parts of your everyday business. Then you should consider whether there are things related to security that are special or different for your business, for which you might need inhouse expertise.

Among routine things, consider how you enforce your corporate policy overall, how you track and audit your finances and business practices, how you manage your relations with employees and customers. What of that can you use to give you a leg up on planning, designing, or building your information security solutions?

Be sure to plan for the cost of hiring and training people for that part of the job you do for yourself. This doesn't necessarily mean you need to hire staff solely for information security. You may, in fact, choose to create a special information security team or department. But you might choose to have your own people do only those aspects of information security that fit well with their other responsibilities. In either case, you, as a business leader, will have to ensure they have the training necessary to understand the requirements of this new responsibility, and to continue to perform the job well.

Using outsiders to do it for you

Once you've decided what you want to do for yourself, you will have to find outsiders who can do the rest. Where should you look? First, look to the companies you do business with on a regular basis. You might be surprised how much assistance you can get from your computer or software vendors, your auditing firm, even your casualty insurance company. Only after you look at your existing business relations should you turn to new partners specifically for help with information security. Here are some suggestions.

Software vendors must be part of your security solution team. Ask your software vendors whether their products are "secure." Since they will almost always say "yes" you will have to be more specific. Ask them about the sort of things we've addressed in this guide. Are the security features contained in the software product itself, or does it rely on or participate in a larger security solution? (Much conventional office software appropriately relies on the operating system to provide its basic security services.)

Ask how the product protects the information it works on, how it recognizes and tailors itself to specific users, and how it protects itself from corruption or misconfiguration. Depending on the business relationship you have with your software vendor, you might ask these questions directly of the vendor's engineers, or you might just review the manual that comes with the product. Take full advantage of whatever opportunity you have to get the answers you need.

Some software vendors can be a source of information regarding other security products and services than the ones they want to sell you. This is especially likely if the vendor is selling products that are security related. Vendors of directories, authorization systems, cryptography packages, fingerprint recognition, and similar products should be in a position to assist you in designing a comprehensive security system.

But let the buyer beware! Most every vendor of security software will claim to have the best and most complete solution for your needs. They can't all be right. Many will offer you products that do not come close to what we have described as "good," "better," and "best" systems. Ask

your vendor if he's read this guide, and how his product compares to what we've described. (If he hasn't read it, give him your copy. Then write to us and tell us the vendor's name and address, and we'll send you a new copy for free!)

Auditors and insurers may be able to provide you with useful guidance about security. More and more, auditors are making security an audit item. Insurers are learning to include the quality of a company's security as a factor in the rate setting process. Over the next few years, auditors and insurers will be developing significant competence in information security. Your auditors and insurers may offer you security advice without your even asking. If they criticize your security solution, don't take offense; take the advice! If they don't critique your security, ask them to.

Consultants and system integrators can be helpful in designing and implementing security systems, even for companies with competent information security staff. If you do your own design and implementation, you should consider having a consultant review the system from an independent perspective. Consulting companies can provide training for you and your staff. Consider training for employees responsible for building and operating your security systems themselves, and also training for your other employees on how and why they should use the security services.

You might rely on a system integrator to help you design and implement your security systems. Systems integrators range from consulting organizations that operate on a global scale to neighborhood computer dealers who supply complete small office automation solutions. When you work with such organizations, be certain they are willing to provide you with what you need, and not just what they have to sell.

When considering candidates, look for consultants and integrators with recent experience securing businesses similar to yours. The individuals performing or supervising the work should have professional certifications that indicate they are current with information security technology.

Remember, it is *your* responsibility to ensure your company's security, not the consultants'. Be sure they remember that it's *your* business. It's *their* obligation to make sure *you* understand what they propose or build, and why. Your goal is to have a security solution that supports your policies, not to reshape your business merely to meet someone else's model of security.

Outsourced security services are provided by companies called "Security Service Providers," or SSPs. Like "Application Service Providers," or ASPs, SSPs take responsibility for operating information systems for their clients. SSPs operate security systems of various sorts. Some focus on specialty areas like intrusion detection, others provide outsourced operation and management of firewalls, web portals, and other elements of a security system.

You may find that, particularly where a function is resource intensive (like scanning and analyzing intrusion audit logs), the use of outsourced services is more cost effective than inhouse operations. You must strike a balance between the economies an outsourced service can provide and your need to tailor your solution exactly to your business. Whatever route you take, make sure your contracts include Service Level Agreements (SLAs) that tell what your SSP will do, what benefit you will get, how that will be measured, and what penalties they get if they don't deliver.

Security of penetration testing is a way to identify gaps in your protection. The practitioners of this sort of testing sometimes style themselves "tiger teams" or "ethical hackers." They try to break in to your systems the way hackers or other adversaries might.

There are differences of opinion about whether and how tests of this sort should be conducted. One concern is that a penetration exercise, if not done with great care, can itself be damaging to the integrity of the systems being tested. If you decide to do this sort of testing, be sure to use a reputable company (after all, they'll learn your weaknesses), and check references. Establish ground rules for the test, and cover yourself with a contract. And remember, just because a penetration test finds no gaps, don't assume there are none.

No company is an island

Whether you've chosen to rely on your own staff or on third parties to handle your security solutions, there are some things that require you to work together with your suppliers and others on a continuous basis. There are a number of reasons for this. First, there is so much to know about information security, you will be wise to rely on others to help you

keep up. Perhaps more important, most or all of your information systems — not just your security systems — will be created by others. They will of necessity be a part of everything you do to keep you systems functioning to meet your needs.

Tracking global threats

Not all threats that could affect your business will be directed specifically at you. Viruses, worms, and other fancifully named bits of malicious software that plague the Internet are not aimed specifically at your business. Most often they are aimed at certain types or brands of software. They may be used in attempts to disrupt economic systems or nations. It will be very difficult for you to assess these threats or create your own protections against them. You will have to rely on virus scanning systems and services to help defend your systems.

Some viruses are created by very ingenious people, who sometimes discover ways to get around the protections that you will likely use. The companies that provide virus protection solutions are also ingenious, and usually have new protections available within hours of the first discovery of a virus. Be sure, if you rely on virus protection software, to subscribe to the update service that will entitle you to the new protections as soon as they are created.

Keeping your software up-to-date

Unfortunately, many software products — even products from major software companies — are delivered with security defects. Sometimes these defects are discovered by the suppliers or their clients in the normal course of business. Sometimes they are only discovered after malicious parties exploit them, sometimes by "hacking" through the defect, sometimes by creating a virus that takes advantage of it.

We would like to be able to tell you that there are vendors of software who will solve this problem, without your needing to do anything. But there aren't. Some suppliers of software will keep you advised of changes that

need to be made over time. Some will provide ways for their products to be updated easily whenever a change is needed to correct a security flaw. It's up to you to take advantage of the services your suppliers offer.

We know that software can be a big expense. Still, you should consider buying a new version from time to time, even if the old version still works for you. Newer versions of software are more likely to have the most current security features. But beware! Sometimes new versions also have new weaknesses. Consider waiting until the version has been on the market for a while before you adopt it.

Be prepared

One last word of caution: no security system will ever be perfect! There will always be a chance that something will go wrong. But that won't surprise you, because everything is like that. You've probably given at least some thought to the possibility that your business might suffer a loss because of fire, flood, or windstorm. If you have, you may have come up with a formal disaster recovery or business continuity plan.

Preparing for a possible information security failure should be no less (and no more) important than preparing for any disaster. The steps that will protect you from one will probably also protect you from the other. Back up your important information regularly, and store it someplace safe — off-site. Know how to bring the information back from storage when you need to. Keep accurate records of all your information technology assets — systems, software, information, and expertise — and know how you could restore or replace them. Just as you have fire drills, have information recovery drills. And, most important, keep your plans and policies up-to-date.

More information

This guide is only an introduction to information security. There's much more you and your staff will want and need to know. It will always be important for you and your staff to stay on top of the latest techniques and issues in information security. For the best source of pointers to up-to-date security information, visit our web site at www.opengroup.org/security/more.htm.

bibliography

The technologies and details of information security are changing rapidly. But the basic principles of using information security for business purposes are fairly constant. It's just good business.

This brief bibliography includes a few background books we have found to be interesting, and that we think will be interesting for you. To find references to more topical or timely material, visit The Open Group's Security Bibliography on the web at www.opengroup.org/security/more.htm.

Books of General Interest

Secrets and Lies: Digital Security in a Networked World
Schneier, Bruce (John Wiley & Sons, 2000) 432pp
An overview of the landscape of digital security, the technologies in use, and approaches to creating effective security soluions.

Time-Based Security
Schwartau, Winn (Interpact, 1999) 192pp
An approach to information security that differs from the usual "fortress mentality" model.

The Code Book
Singh, Simon (New York: Doubleday, 1999) 402pp
A history of the use of cryptography and secret writing from ancient times to the present.

Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage
Stoll, Clifford (New York: Pocket Books, 2000) 402pp
The classic story of a search for a cybercriminal.

index

Page numbers in bold type show the page where the word or expression is defined.

About the Author

Eliot M. Solomon has been a leader in the practical use of infrastructure technology in the solution of real business problems, with special emphasis on the problems of the Securities Industry.

In fifteen years with the Securities Industry Automation Corporation (SIAC) he was intimately involved in designing and implementing systems supporting major organizations of the Securities Industry. He was responsible for the creation of new technology strategies and the application of emerging technologies in support of SIAC and its customers.

Eliot is widely known in Wall Street's technology community as a result of his active participation in The Open Group, the Securities Industry Middleware Council (SIMC), and other industry organizations. He is a cofounder of SIMC and has served as its president since 1998. As a member of The Open Group, Eliot chaired the DCE Program, and has been a member of the steering committee of the Security Forum.

Before turning his attention to Wall Street, Eliot worked in medical electronics, telecommunications, and defense systems.

Manager's Guide to Information Security

Information security is increasingly vital for businesses of all sorts. The objective for business managers when they purchase or build security solutions for their business is to make choices that make business sense. But the subject is obscured by technical jargon, fear mongering, and, too often, a desire by practitioners of security technology to impress rather than inform.

In the Manager's Guide to Information Security, Eliot Solomon and the Security Forum of The Open Group provide a no-non-sense guide to the use of information security technology in a real business. It explains what is needed – and what isn't – and why. It emphasizes opportunities to "use what you have", minimizing the cost and maximizing the value of IT security purchases. And most important, it presents security technology as a way to address real business policy.

THE *Open* GROUP

- 44 Montgomery St., Suite 960
  San Francisco, CA 94104 USA
  Tel +1.415.374.8280
  Fax +1.415.374.8293
  (USA Sales Only)
  1.800.916.OPEN (6736)
- 29B Montvale Avenue
  Woburn, MA 01801
  Tel +1.781.376.8200
  Fax +1.781.376.9358
- Apex Plaza, Forbury Road
  Reading, Berkshire RG1 1AX, UK
  UK Free Phone
  (0)800.072.9490
  Tel +44 (0)118.950.8311
  Fax +44 (0)118.950.0110

US $9.99 G250

ISBN 1-931-62406-2 90000

9 781931 624060