GETTING STARTED
Information security is not just about technological controls. Security cannot be achieved solely through the application of software or hardware. Any attempt to implement technology controls without considering the cultural and social attitudes of the corporation is a formula for disaster. The best approach to effective security is a layered approach that encompasses both technological and nontechnological safeguards. Ideally, these safeguards should be used to achieve an acceptable level of protection while enhancing business productivity. While the concept may sound simple, the challenge is to strike a balance between being too restrictive (overly cautious) or too open (not cautious enough).

Security technology alone cannot eliminate all exposures. Security managers must integrate themselves with existing corporate support systems. Together with their peers, they will develop the security policies, standards, procedures, and guidelines that form the foundation for security activities. This approach will ensure that security becomes a function of the corporation — not an obstacle to business.

A successful layered approach must look at all aspects of security. A layered approach concentrating on technology alone becomes like a house of cards. Without a foundation based on solid policies, the security infrastructure is just cards standing side by side, with each technology becoming a separate card in the house. Adding an extra card (tech-
nology layer) to the house (overall security) does not necessarily make the house stronger.

Without security policies, standards, procedures, and guidelines, there is no general security framework or foundation. Policies define the behavior that is allowed or not allowed. They are short because they do not explain how to achieve compliance; such is the purpose of procedures and guidelines. Corporate policy seldom changes because it does not tie to technology, people, or specific processes. Policy establishes technology selection and how it will be configured and implemented. Policies are the consensus between people, especially important between all layers of corporate management. Policy can ensure that the Security Manager and his or her peers apply security technology with the proper emphasis and return on investment for the good of the business as a whole.

In most security audits or reviews, checking, maybe even testing, an organization's security policies, standards, procedures, and guidelines is often listed as the first element in assessing security risk. It is easy to see the published hard-copy policy; but to ensure that policy is practiced, it is necessary to observe the workplace in order to evaluate what is really in operation. Lack of general awareness or compliance with a security policy usually indicates a policy that was not developed with the participation of other company management.

Whether the organization is global or local, there is still expectation of levels of due diligence. As a spin on the golden rule: “Compute unto others as you would want them to compute unto you.”

Define the Scope: Objective

“The first duty of a human is to assume the right functional relationship to society — more briefly, to find your real job, and do it.”

— Charlotte Perkins Gilman

Define Security Domain

Every organization has a different perspective on what is within the domain of its Information Security department.

- Does the Information Security domain include both electronic and non-electronic information, printed versus the bytes stored on a computer?
- Does the Information Security department report to IS and have responsibility for only information policies, not telephone, copier, fax, and mail use?
- Does physical security and contingency planning fall into the Information Security Manager’s domain?
- Is the Security Manager’s responsibility corporate, regional, national, or global?
Information Security’s mission statement must support the corporation’s business objective. Very often, one can find a security mission stated something like:

> The mission of the Information Security department is to protect the information assets, the information systems, and networks that deliver the information, from damage resulting from failures of confidentiality, integrity, and availability (CIA) (see Exhibit 1).

This mission is quite specific to Information Security and a specific department. A mission like this is a prime reason why defining the Security Manager’s domain is critical to the success of policy formation.

Would the mission be more positive and clear by being tied to the business objectives with something like:

> Security’s objective is to enhance the productivity of the business by reducing probability of loss through the design and implementation of policies, standards, procedures, and guidelines that enhance the protection of business assets.

Notice how this mission statement does not limit itself to “information.” It does not limit the responsibilities to only computer systems and their processing of information. In addition, it ties the success of the mission to the business. It still provides the flexibility to define assets and assign owners to them for accountability. It is important to understand the objectives that security is going to deliver for the business. Exhibit 2 outlines some sample objectives.
What will be in the Security Manager’s domain: physical security, contingency planning, telephones, copiers, faxes, or mail (especially e-mail)? These technologies process information too, so would they be covered by Information Security Policy? How far reaching will the Security Manager’s responsibilities be: corporate, global, national, regional, or local? Is it the Security Manager’s responsibility to enforce compliance? Is contingency planning or business continuity planning (BCP) a function of physical security? Once the domain has been clearly defined, it becomes easy for responsible areas to form and begin to create their specific policies, standards, procedures, and guidelines.

Traditionally, organizations would refer to different departments for the responsibility of security on such things as telephones, copiers, faxes, or mail. An organization would have to climb quite high in the organizational structure — executive VP, COO, CEO — to find the common management point in the organizational structure where a person responsible for the security of all the disparate resources would come together for central accountability.

Hint: Policies written with the term “electronic” can cover e-mail, (electronic mail), EDI (electronic data interchange), or all the other “E-words” that are becoming popular (i.e., E-commerce, E-marketing, and E-business). Policies not using the term “electronic” can refer to information regardless of technology, storage media, or transportation methods.

In that regard, what used to be called datasecurity, today is referred to as information security. Information security often considers the security of data, information in both electronic and non-electronic forms. The role of the Information Security Manager has either expanded or information security personnel have begun assuming responsibilities in areas that are

---

**EXHIBIT 2 — Questions to Help Determine Security Philosophy**

- Do users have expectations relating to security?
- Is it possible to lose customers if security is too restrictive, not restrictive enough, or if controls and policy are so unreasonable that functionality is impaired?
- Is there a history for lost availability or monetary loss from security incidents in the past? What was the cost to the business?
- Who is the primary enemy — employees or outsiders?
- How much confidential information is online, and how is it accessed? What would be the loss if the information was compromised or stolen?
- Is it important to layer security controls for different parts of the organization?
- Are dangerous services that increase vulnerabilities supported by the organization?
- Is it required that networks and systems meet a security baseline?
- What security guidelines, procedures, regulations, or laws must be met?
- Is there a conflict between business objectives and security?
- Confidentiality, integrity, and availability: how crucial is each to the overall operation?
- Consider business needs and economic reality. What meets due diligence for like companies, the security industry, for this information in other environments?
often not clearly defined. Some organizations are recognizing the difficulty of separating information dealing with technology from non-technology. With that in mind, Corporate Security Officer (CSO) type positions are being created (other possible name: Chief Security Officer). These positions can be scoped to have responsibility for security, regardless of technology, and across the entire enterprise regardless of geography. This would not necessarily mean that all of the impacted areas report to this position, but this position would provide the enterprise or corporate vision of information security. It would coordinate the security accomplishments for the good of the entire organization, crossing domains and departments. Define “information”; what does it not include?

For years, security purists have argued for information security to report high in the organization as well as not necessarily within the information services (IS) division. Some organizations accomplished this by creating executive-level security positions reporting to the president, COO, or CEO. In differing ways, more organizations are finally making strides to at least put the “corporate” or “enterprise” spin on addressing the security issues of the organization, not just the issues (policy) of IS. An appointment of security personnel with accountability across the organization is a start. Giving them top management and line management support across the organization remains critical to their success, regardless of how high they report in the organization. An executive VP of information security will fail if the position is only a token position. On the other hand, the flunky of information security can be successful if everyone from top down is behind him and the concept of corporate information security.

In this structure, traditional areas can remain responsible for their parts of security and policy definition, their cards in the house, but a corporate entity coordinates the security efforts and brings it all together. That corporate entity is tasked with providing the corporate security vision and could report high in the organization, which is probably the best, or it could be assigned corporate responsibility by executive management. Total and very visual support by all management is obviously critical for success.

Sample roles and responsibilities for this structure include:

- The protection and safety department would continue to contract for guards, handle building access control, ID cards, and other physical building controls, including computer rooms.
- The telecommunications department is still be accountable for the security of phone systems and helps with establishment of policy addressing phone-mail and use of company telephones, probably including fax.
- A corporate mail department deals with internal and external mail, possibly including e-mail.
• IS has accountability for computer-based information processing sys-
tems and assists with the establishment of standards for use of them
or policy dealing with information processing.
• The corporate legal department would help to ensure that policy
meets regulations from a legal perspective and that proper wording
makes them enforceable.
• A corporate compliance department can insure that regulatory and
legislative concerns are addressed, such as the federal sentencing
guidelines.
• Human resources (HR) is still a critical area in identifying employee
policies and works closely with the Corporate Security Officer (CSO)
on all policies, standards, procedures, and guidelines, as well as
proper enforcement.
• The CSO works with all areas to provide high-level security expert-
tise, coordinate and establish employee security awareness, security
education programs, along with publication and communication of
the security policies, standards, procedures, and guidelines.

SECURITY PHILOSOPHY

No gain is possible without attendant outlay, but there will be no profit if the
outlay exceeds the receipts.

— Plautus

Return on Investment (ROI): What is the basis for security philosophy?
Security is often expected to provide a return on investment (ROI) to jus-
tify expenditures. How often is it possible for information security to
generate a direct ROI? Which is more expensive, recover from an inci-
dent or prevent the incident in the first place? Computer security is often
an intangible process. In many instances, the level of security is not evi-
dent until a catastrophe happens, at which time the lack of security is all
too painfully evident.

Information security should be viewed in terms of the processes
and goals of the business. Business risk is different from security risk,
but poor security can put the business at risk, or make it risky doing
business.

Examples.
• Would a wise company provide banking services, transmitting credit
card numbers and account balances using an unsecured Internet
connection? A properly secured infrastructure using encryption or
certificates for nonrepudiation can provide the company with a busi-
ness opportunity that it would not otherwise be likely to engage in.
In that situation, the security is an integral part of that business op-
portunity, minimizing the business risk.
• How can a security manager justify control procedures over program changes or over developers with update access to production data? Assume that 20 percent of problems result from program errors or incorrect updates to data. Maybe inadequately tested code in a program is transferred to production. If controls can reduce the errors and resulting rework to say 10 percent, the payback would be only a few months. In a company that sells its programming services based on quality, this would directly relate to potential business opportunity and increased contracts.

• What about customer privacy? A Harris Poll showed that 53 percent of American adults are concerned about privacy threats from corporations. People have stated in surveys that they would rather do business with a company they feel is going to protect the privacy of their information. Increased business opportunity exists for the company that can show that it protects customer privacy better than its competition, even if it only generates the perception of better. Perception is 90 percent reality. Being able to show how the company enforces sound security policies, standards, and procedures would provide the business advantage.

Although a mission statement may no longer refer directly to confidentiality, integrity, and availability, the security department cannot ignore CIA (see Exhibit 1). As discussed, the base security philosophy must now help improve business productivity. The real life situation is that we can never provide 100 percent security. We can, however, reduce the probability of loss or taking reasonable measures of due diligence consistent with industry norms for how like companies are dealing with like information. Going that extra step ahead to lead the industry can create business opportunity and minimize business risk.

To meet the security business objective, a better order for this triad is probably AIC, but that does not stir as much intrigue as CIA. Studies show AIC to be better matched to the order of priority for many security managers.

Why?

• Availability: A corporation gathers endless amounts of information and in order to effectively produce product, that information must be available and usable when needed. This includes the concept of utility, or that the information must have the quality or condition of being useful. Just being available is not sufficient.

• Integrity: For the information to have any value and in order to produce quality product, the data must be protected against unauthorized or inadvertent modification. Its integrity must be of the highest
quality and original. If the authenticity of the information is in doubt or compromised, the integrity is still jeopardized.

- **Confidentiality:** The privacy of customer information is becoming more and more important, if not to the corporation, to the customer. Legislation could one day mandate minimum protections for specific pieces of information like health records, credit card numbers, and bank account numbers. Ensuring that only the proper people have access to the information needed to perform their job or that they have been authorized to access it is often the last concern because it can impede business productivity.

**MANAGEMENT MYTHS OF SECURITY**

1. Security technology will solve all the problems.

   Buy the software; now the company is secure. Management has signed the purchase order and the software has arrived. Is management’s job finished and the company now secure? Management has done their due diligence, right? Wrong! Remember, software and security technologies are only a piece of the overall security program.

   Management must have a concept or philosophy regarding how it wants to address information security, recognizing that technology and software are not 100 percent effective and are not going to magically eliminate all security problems. Does the security software restrict any access to a resource, provide everyone access, or just audit the access until someone steps forward with resources that need to be protected? The security job is not done once the software is installed or the technology is chosen.

   Management support for proper security software implementation, configuration, continued maintenance, and the research and development of new security technologies is critical.

2. I have written the policy, so now we are done.

   If policies or standards are written but never implemented, or not followed, not enforced, or enforced inconsistently it is worse than not having them at all. Federal Sentencing Guidelines require consistent application of policy and standards.

   In an excerpt from the Federal Sentencing Guidelines, it states:

   > The standards must have been consistently enforced through appropriate disciplinary mechanisms, including as appropriate, discipline of individuals responsible for the failure to detect an offense. Adequate discipline of individuals responsible for an offense is a necessary component of enforcement; however, the form of discipline that will be appropriate will be case specific.

   Management must recognize that policy and standards implementation should be defined as a specific project receiving continued management support. They may not have understood that there is a cost
associated with implementing policy and thought this was only a policy development effort.

Strict enforcement of policy and standards must become a way of life in business. Corporate policy-making bodies should consider adherence to them a condition of employment. Never adopt a policy unless there is a good prospect that it will be followed. Make protecting the confidentiality, integrity, and availability of information “The Law.”

3. Publish policy and standards and everyone will comply.

Not only is the job not done once the policy is written, but ensuring that every employee, customer, vendor, constituent, or stockholder knows and understands policy is essential. Training them and keeping records of the training on company policy are critical. Just publishing the policy does not encourage anyone to comply with it.

Simply training people or making them aware (security awareness) is also not sufficient; all one gets is shallow or superficial security. There needs to be motivation to carry out policy; only penalizing people for poor security does not always create positive motivation and is a militaristic attitude. Even child psychologists recommend positive reinforcement.

Security awareness alone can have a negative effect by teaching people how to avoid security in their work. Everyone knows it just slows them down, and they hate it anyway, especially if only penalties are associated with it. Positive reinforcement calls for rewards when people show actions and attitudes toward very good security. Do not eliminate penalties for poor security, but do not let them be the only motivator. Once rewards and penalties are identified, education can include how to achieve the rewards and avoid the penalties, just as for other work motivation. This requires an effectively applied security line item in salary and performance reviews and real rewards and penalties.

4. Follow the vendor's approach: it is the best way to make an organization secure.

An organization’s goals should be to build the fences as high as it can. Protect everything; implement every feature of that new software. The organization has paid for those functions and the vendor must know the best way to implement them.

Often, an organization might be inclined to take a generic security product and fail to tailor it to fit its business objectives. Everyone can name an operating system that is not quite as secure as one would like it to be using the vendor defaults. The vendor’s approach may go against organization security philosophy. The product may come out of the box with limited security, open architecture, but the company security philosophy is to allow only access as appropriate, or vice versa.

Should one put all one’s eggs in one basket or build one’s house all from the same deck of cards? Does using only one security solution from
a single vendor open vulnerability to the security architecture? Think about using the best-of-class solution from multiple vendors; this way, one’s security architecture is not easily blueprinted by outsiders.

BUILDING THE BRIDGE: SECURITY CONTROLS REACH FOR BUSINESS NEEDS

An information security infrastructure is like a bridge built between the user with a business need to access information and at the other end of the bridge the information they wish to access. Creating gates between the end user and the data are the controls (technology) providing security protection or defining specific paths to the information. Forming the foundation for the security technology to be implemented are policies, standards, and procedures.

Guidelines are not required actions, but provide a map (suggestions of how to comply) or, like the railings of the bridge, help direct end users to their destination so they do not fall off the bridge. Just like the rails of a bridge, if the guidelines are not followed, it is still possible to fall off the bridge (not comply with policy and standards). The river represents unauthorized access, malicious elements (hackers), or unauthorized entities (disgruntled employees) that could affect the delivery of the payloads (information) across the bridge. The river (malicious access) is constantly flowing and often changing faster than security controls can be implemented. The security technology or software are locked gates, toll ways, or speed bumps on the bridge that control and audit the flow of traffic authorized to cross. Exposures or risks that have been accepted by management are represented by holes in the surface of the bridge that are not patched or are not covered by a security technology. Perhaps they are only covered with a see-through mesh, because ignorance is the only protection. The bigger the risk, the bigger the hole in the roadbed.

Build bridges that can get the organization from the “Wild Wild West” of the Internet to the future wars that are yet to be identified. William Hugh Murray of Deloitte and Touche once stated that one should build a solid infrastructure; the infrastructure should be a foundation that will last for 30 years. Work to build a bridge that will handle traffic for a long time and one will have the kind of infrastructure that can be depended upon for many years. Well-written and management-accepted policy should rarely change.

THE RIVER: UNDERSTANDING THE BUSINESS NEED

Understanding what one is protecting the business against is the first place to start. Too often, IS people will build a fantastic bridge — wide, double decked, all out of the best steel in the world — then they begin looking for a river to cross. This could also be called knowing the enemy or, in a more positive light to go with the business concept, understanding the business need.
If the Security Manager does not understand what objectives the end users of the information have, one will not know what is the best security philosophy to choose. One will not know whether availability is more important than integrity or confidentiality, nor which should get the primary focus. It will be difficult to leverage sufficient security technology with administrative procedures, policies, and standards. ROI will be impossible to gauge. There will be no way of knowing what guidelines would help the end user follow policy or work best with the technology. Organizations often focus efforts on technical priorities that may not even be where the greatest exposures to the information are (see Exhibit 3). Problems for nonexistent exposures will be getting solved; a bridge will be getting erected across a dry river.

**LAYING THE ROADBED: POLICY AND STANDARDS**

The roadbed consists of policy and standards. Security policy and standards must have muscle. They must include strong yet enforceable statements, clearly written with no room for interpretation, and most importantly must be reasonable and supported by all levels of management. Avoid long or complex policies. As a rule of thumb, no policy should be more than one page in length; a couple of short paragraphs is preferable. Use words in the policy like must, shall, and will. If a policy is something that will not be supported or it is not reasonable to expect...
someone to follow it to do their job, it should not be published. (See also Exhibit 5.) Include somewhere in policy documentation of the disciplinary measures for anyone who does not comply. Procedures and guidelines can provide detail explaining how personnel can comply. To be valid, policy and standards must be consistently enforced. More information on the structure of policy and standards is available later in this article.

Enforcement procedures are the edges of the roadbed. Noncompliance might result in falling off the bridge, which many can relate to being in trouble, especially if one cannot swim. Enforcement provides the boundaries to keep personnel on the proper road. A sample of a simple enforcement procedure for a security violation might be:

1. On the first occurrence, the employee will be informed and given a warning of the importance to comply with policy.
2. On the next occurrence, the employee's supervisor will be contacted. The supervisor will discuss the indiscretion with the employee.
3. Further violations of the same policy will result in disciplinary actions that might consist of suspension or possible termination, depending on the severity of the incident.

In any case, it might be necessary to publish a disclaimer stating that depending on the severity of the incident, disciplinary actions can result in termination. Remember that, to some degree, common sense must come into the decisions regarding how enforcement procedures should be applied, but they should always be consistently enforced. Also, emphasize the fact that it is all management's responsibility to enforce policy, not just the Security Manager's.

Start with the basics, create baselines, and build on them until one has a corporate infrastructure that can stand years and years of traffic. Policy and standards form the benchmarks or reference points for audits. They provide the basis of evidence that management has acted with due diligence, thus reducing their liability.

THE GATE KEEPERS: TECHNOLOGY
Technology is everywhere. In the simplest terms, the security technology consists of specific software that will provide for three basic elements of protection: authentication, accountability, and audit. Very specific standards provide the baselines for which technology is evaluated, purchased, and implemented. Technology provides the mechanism to enforce policies, standards, and procedures.

Authentication. Authentication is the process by which access is established and the system verifies that the end user requesting access to the information is who they claim to be. The process involves providing
one's personal key at the locked gate to open it in order to be able to cross the bridge using the path guarded by that gate.

**Accountability.** Accountability is the process of assigning appropriate access and identification codes to users in order for them to access the information. Establishing audit trails is what establishes accountability.

An example of accountability in electronic commerce is the assignment of digital certificates that can provide varying levels of guaranteed accountability (trust). At the least trusted levels, the user has a credit card or cash to buy a certificate. At a middle degree of trust, there is more checking done to validate that the user really is the person who they claim to be. At the highest level of trust, an entity is willing to stand behind the accountability of the certificate assignment to make it legally binding. This would mean a signature document was signed in person with the registrant that assigns certificates for establishing the accountability.

Assigning a personal key to an individual who has provided beyond-doubt proof (DNA test) that they are who they say they are and that they have agreed to guard their key with their life and that any access by that key can only be by them.

**Audit.** This is the process, on which accountability depends that can verify using system events to show beyond a reasonable doubt, that specific activities, authorized or unauthorized, occurred in the system by a specific user identification at a given point in time. The information is available on request and used to report to management, internal and external auditors, and could be used as legal evidence in a criminal prosecution.

Having the necessary proof that the personal (authentication) key assigned (accountable) to Ken M. Shaurette was used to perform an unauthorized activity such as to modify the payroll system, adding bonus bucks to the salaries of all CISSP personnel.

**PROVIDING TRANSPORTATION: COMMUNICATION**

Communication is the #1 key to the success of any security infrastructure. Not only do policy, standards, procedures, and guidelines need to be communicated, but proper use and availability of the security technologies and processes also need to be communicated. Communications is like the racecar or the bus that gets the user across the bridge faster from their business need to the information on the other side. Arguably, the most important aspect of security is informing everyone that they have a responsibility for its effectiveness.

CERT estimates that 80 percent of network security intrusions are a result of users selecting and using passwords that are easy to guess and as such are easy to compromise. If users are unaware that bad password se-
lection is a risk, what incentive is there to make better selections? If they knew of guidelines that could help them pick a more difficult password to compromise, would they not be more inclined to do so? If users are unaware that guidelines exist to help them, how can they follow them?

**What makes up communications?** Communications involves integrating the policy into the organization using a successful security-training program consisting of such things as:

- new employee orientations
- periodic newsletters
- intranet Web site
- electronic announcements (i.e., banners, e-mail)
- CBT course
- technology lunches, dinners
- informal user group forums
- regular company publications
- security awareness days
- ethics and appropriate use agreements signed annually

**EXPERT VERSUS FOOL: IMPLEMENTATION RECOMMENDATIONS**

Before beginning policy and standard development, understand that in an established organization, policy and standards may exist in different forms. There is probably official, de jure, less official, *de facto* and proprietary, no choice. Official is the law; they are formal and already accepted. Less official consists of things that get followed but are not necessarily published, but maybe should be. Proprietary are the items that are dictated by an operating system; for example, MVS has limitations of eight-character user IDs and eight-character passwords.

**Be the Expert: Implementation Recommendations**

Form a team or committee that gets the involvement and cooperation of others. If the policies, standards, procedures, and guidelines are to become enterprisewide, supported by every layer of management, and be reasonable and achievable, representation from all areas — both technology and non-technology — will go a long way toward meeting that goal. Only a team of the most wise and sage experts from all over the organization will know what may already exist and what might still be necessary.

As the security professional, efforts should be concentrated on providing high-level security expertise, coordination, recommendations, communication, and education in order to help the team come to a consensus. Be the engineer, not the builder; get the team to build the bridge.
Layering Security

Layer protection policies and standards. Support them with procedures and guidelines. Review and select security technology that can be standards. Create guidelines and procedures that help users comply with policy. Establishing policy and adequate standards provides the organization with control of its own destiny. Not doing so provides the potential for auditors (internal or external) or legal actions to set policy.

The following walks the reader through the layers outlined in Exhibit 4, from the top down.
Corporate Security Policy. This is the top layer of Exhibit 4. There should be as few policies as possible used to convey corporate attitude and the attitude from the top down. Policies will have very distinct characteristics. They should be short, enforceable, and seldom change. See Exhibit 5 for tips on writing security policy. Policy that gets in the way of business productivity will be ignored or eliminated. Corporate ethics are a form of policy at the top level. Proper use of computing resources or platforms is another example of high-level policy, such as the statement, “for business use only.”

EXHIBIT 5 — Tips on Writing Security Policy

1. Make the policy easy to understand.
2. Make it applicable. Does the policy really fit? Does it relate to what actually happens at the company? Does it fit the organization’s culture?
3. Make it do-able. Can the company still meet business objectives if the policy is implemented?
4. Make it enforceable.
5. Use a phased-in approach. Allow time for employees to read, digest, and respond to the policy.
7. Avoid absolutes; almost never say “never.”
8. Use wording such as “must,” “will,” or “shall” — not “would,” “should,” or “could.”
9. Meet business objectives. Allow the organization to identify an acceptable level of risk.
10. Address all forms of information. (How were the machine names obtained)?
11. Obtain appropriate management support.
12. Conform. It is important that policy looks like other written company policies.
13. Keep it short. Policies are shorter than procedures or practices, usually one or two pages in length maximum.
14. What is to be protected?
15. When does the policy take effect?
16. Where within the organization does the policy reach? Remember the scope.
17. To whom does the policy apply? Is there a limitation on the domain?
18. Why was the policy developed?
19. Who is responsible for enforcement?
20. What are the ramifications of noncompliance?
21. What, if any, deviations are allowed? If allowed, what are the deviation procedures?
22. Are audit trails available and required?
23. Who developed, approved, and authorized the policy?
24. How will compliance be monitored?
25. Are there only penalties for noncompliance, or are rewards available to motivate people toward good practices?
26. Who has update and maintenance responsibility for the policies?
27. How often will the policy be reviewed and updated if necessary?
28. Are there documented approval procedures for new or updated policy?
29. Is there an archive of policy, past to present? What was in effect last year at the time of the incident?
30. What is the date of the last revision?
SAMPLE POLICY:
Information will be protected based on a need-to-know philosophy. Information will be classified and protected in a manner commensurate with its sensitivity, value, and criticality. Protection of information will apply regardless of the media where the information is stored (printed, electronic, etc.), the systems that process it (PC, mainframes, voice mail systems, etc.), or the transport mechanisms by which it is moved (fax, electronic mail, TCP/IP network, voice conversation, etc.).

Functional Standards. Functional standards (the second layer of Exhibit 4) are generally associated to a business area. The Loan department in a bank might have standards governing proper handling of certain loan information. For example, a loan department might have a standard with an associated procedure for the special handling of loans applied for by famous people, or executives of the company. Standards might require that information assigned sensitive classification levels is shredded, or an HR department might require that employee profiles only be printed on secure printers, available and handled only by specific personnel. The Claims department in an insurance company may set standards that require the printing of claim checks on printers local to the office that is handling the claim.

Computing Policy. The computing policies (the third layer in Exhibit 4) are tied with technology. These standards establish computing environments such as identifying the standard security software for securing mainframe-computing environments (i.e., CA-Top Secret, RACF, or CA-ACF2), establishing an encryption standard (i.e., PGP, BLOWFISH, DES, 3DES) for every desktop/laptop, or transmission of any sensitive information. Information services is most likely establishing the computing security standards that work with information owner requirements, and business needs.

Security Baselines. Security baselines (the fourth layer in Exhibit 4) can also be called the minimums. These are tied very closely to the operating environment and day-to-day functioning of the business. Some baselines might be password expiration intervals, password content controls (six characters must be one numeric or special character), and minimum length of user ID. Another might be requiring that every computing system perform authentication based on a personal identity code that will be assigned to each user and that they use their personal password or alternative authentication (token, biometrics) before access is granted to perform any activities. Audit would also be another baseline requirement.

Technology and Physical Security. Technology and physical security are the components making up the bottom layer of Exhibit 4. This
is the technology, the security software or hardware, that makes up the various computing platforms that comprise the information processing environment. It is the specific security within an NOS, an application, firewalls for the network, database security, or any other specific technology that provides the actual controls that allow the organization to enforce baselines and standards. An application program may have the security checking that restricts the printing of employee profiles and claim checks or provides alerts and special handling controls for loans by special people.

**Procedures and Guidelines.** Procedures and guidelines cross all layers of the information security infrastructure, as illustrated in Exhibit 4. Guidelines are not required actions, but procedures could fall into either something that must be done or provide help in compliance with security policy, standards, and technology. The best policy and standard can have minimal value if people do not have guidelines to follow. Procedures go that next step in explaining the why and how of policy in the day-to-day business operation to help ensure proper implementation and continued compliance. Policy can only be concise if the guidelines and procedures provide sufficient explanation of how to achieve the business objective. Enforcement is usually spelled out in the form of a procedure; procedures would tell how to and why it is necessary to print to specific printers or handle certain loans in a special way. Guidelines are the hints and tips; for example, sharing one’s password does not eliminate one’s accountability; choose passwords that are not easily guessed and give sample techniques for password selection. Help personnel find the right path and they will follow it; reminders of the consequences are good incentives.

**THE POLICE ARE COMING!**

In conclusion, what are the measures that can be taken to protect the company or management from litigation? Security cannot provide 100 percent protection. There will be a need to accept some risk. Recognize due care methods to reduce and limit liability by minimizing how much risk must be accepted. Computer security is often an intangible process. In many instances, the level of security is not evident until a catastrophe happens, at which time the lack of security is all too painfully evident. Make the protection of corporate information assets “the law.” Make adherence to policy and standards a condition of employment. Policy, standards, and procedures must become part of the corporation’s living structure, not just a policy development effort. Information security’s objective is to enhance the productivity of the business by reducing probability of loss through the design and implementation of policies, standards, procedures, and guidelines that enhance the protection of business assets.
• Information security is not just about technological controls such as software or hardware. Establishing policy and adequate standards provide an organization with control over its own destiny.
• Information security should be viewed in terms of the processes and goals of the business. Business risk is different than security risk, but poor security can put the business at risk; or make it risky doing business.
• Security must become a function of the corporation, and not viewed as an obstacle to business. Policies support the business; put them in business terminology.
• Form a team. Only a team of the most wise and sage experts from all over the organization will know what policy may already exist and what might still be necessary.
• There should be as few policies as possible used to convey corporate attitude and the attitude from the top down. Policies will have very distinct characteristics. They should be short, enforceable, and seldom altered. They must include strong yet enforceable statements, be clearly written with no room for interpretation, and most importantly, must be reasonable and supported by all levels of management. Use words in the policy like must, shall, and will.
• Policy can only be concise if the guidelines and procedures provide sufficient explanation of how to achieve the business objective.
• Test policy and standards; it is easy to know what is published, but is that what is really in operation?
• To be valid, policy and standards must be consistently enforced.
• Carefully define the Security Manager’s domain, responsibility, and accountabilities. Clearly identify the scope of their job.
• Communication is the #1 key to the success of any security infrastructure.

  To defeat a strong enemy: Deploy forces to defend the strategic points; exercise vigilance in preparation, do not be indolent. Deeply investigate the true situation, secretly await their laxity. Wait until they leave their strongholds, then seize what they love.

  — Sun Tzu

Information security is a team effort; all members in an organization must support the business objectives; and information security is an important part of that objective.

Ken Shaurette, CISSP, CISA, is a senior systems engineer working on security and audit projects for the Multi-User Server Team at American Family Insurance in Madison, Wisconsin. He has more than 20 years' experience in the computer industry. An information security professional since 1985, Ken has experience in writing and conducting security and audit reviews. Ken has written articles and provided training on security and audit issues, which help improve a company’s resistance to unauthorized modification and disclosure of information resources.