INTRODUCTION
The missing factor in an effective information protection program is employee involvement. Many organizations go to great lengths to develop an extensive set of controls and countermeasures, purchase the latest technology, design in audit trails, and print out security logs, and still security fails. Often times this is the result of not understanding the culture and direction of the organization and its employees. To assist in the development of an effective information protection program, it is necessary to examine war stories to see where controls failed in other organizations. There are six key elements that lead to the breakdown of an information protection program. This article will examine them and provide means to resolve the dilemma.

WHY ARE CONTROLS NEEDED?
The legal obligations of senior management fall into two categories: a duty of loyalty and a duty of care. By assuming office, the organization director commits allegiance to the enterprise and acknowledges that the best interest of the corporation and its shareholders must prevail over any personal, individualized interest. This is known as the duty of loyalty.

In addition to owing a duty of loyalty to the corporation, senior management also assumes a duty to act carefully in fulfilling the important tasks of monitoring and directing the activities of corporate management. The Model Business Corporation Act, which has been adopted in whole or in part by a majority of states, reflects the fact that a corporation acts through the individuals who act on behalf of the corporation. This article examines the reasons security in an organization breaks down, and provides possible solutions.
its behalf. These individuals, in executing the corporate mission, are subject to the sanctions that govern the corporation. Shareholders, as well as the corporation itself, place their trust and confidence in corporate leaders. Directors and officers, therefore, are expected to exercise due care in conducting business on behalf of the corporation.

The liability for aiding a corporation in such acts as patent, copyright, or trademark infringements, can fall directly upon its directors and officers. Corporate white collar crime is the specific focus of the Federal Guidelines for Sentencing for Criminal Convictions. Whenever it is necessary to apply these guidelines, consideration is given to organizations that have implemented an effective program to prevent and detect violations of the law.

Additionally, directors and officers are charged with responsibility for the management and protection of corporate assets. This area of responsibility is governed principally by the laws of the state under which the corporation is formed.

An effective information protection program is measured by whether the organization exercised due diligence in seeking to prevent and detect criminal conduct by its employee and other agents. In the event of a security breach, corporate officers must be able to show that reasonable care could avert charges of negligence.

IMPACT ON PROFIT AND LOSS
Exercising due care can also have a direct impact on the profitability of a corporation. An ineffective or nonexistent internal controls program will leave an enterprise vulnerable to the misappropriation of corporate assets. For example, the 1995 National Retail Security Survey reported that retailers lost $27 billion to a combination of employee and customer theft. A full 20% (about $5.4 billion) of this loss was due to administrative error. An effective loss prevention program, part of an overall corporate security program, should be maintained to address this issue. A loss prevention program, specifically designed to control the loss of physical inventory, includes measures such as cabling devices to secure equipment and inventory sensor tags that trigger an alarm when passing through a portal. One of four companies suffered financial losses, often exceeding $100,000 and sometimes $1 million, due to information security breaches, according to a recent Ernst & Young survey of top information systems executives.

Laxness in regard to due care can be costly in other ways as well. The Business Software Alliance (BSA) is running a campaign that encourages employees to call their 800 number and turn in their bosses for copyright infringement. A disgruntled former employee of an automobile manufacturer provided such a tip and the company ended up paying a $260,000 settlement to BSA for copyright abuse. In this instance, top management
indicated that they were unaware of the infringement, the company was still liable for the fine, and had to agree to replace unlicensed software with legal software.

ELEMENTS OF AN EFFECTIVE PROGRAM

A key to demonstrating due care is the implementation of a comprehensive security program. This would include clearly defined responsibilities that are communicated to all employees. The cornerstone to this would be documented security policies and procedures that include discussions on proprietary information, patents, and copyrights.

Access control measures must be implemented to protect information, financial, proprietary, intellectual, and physical assets of the corporation. Because information is present throughout the organization, these controls would have to encompass more than just mainframe concerns. Information, wherever it is resident, will have to be addressed and protected. Access control to workstations, E-mail messages, electronically held files, printed documents, and even the trash will have to be addressed.

A comprehensive business continuity plan (BCP) is another integral element of a corporate security program. A BCP goes beyond the traditional data center disaster recovery plan and includes the entire campus facility. Preventative measures such as fire suppression, emergency response procedures, data backup requirements, and recovery procedures to expedite the speedy return of normal operations are all part of an effective BCP.

Monitoring compliance to established security policies and procedures is another measure in a comprehensive information protection program. Establishing auditing and monitoring procedures, including checklists of items to be scrutinized during a review, will facilitate this process and demonstrate an organization's intent to exercise due care as it conducts its business.

NEED TO CONTROL ALL “EMPLOYEES”

Contractors and consultants should receive information only if it is relevant to their assignment. There should be a general awareness among internal employees concerning this limitation on access. If contractors are working on long-term projects, diligence tends to grow lax. Nondisclosure agreements (confidentiality agreements) should be signed by all contractors upon hire and should be reviewed with them upon termination, as a reminder. If the contractor's project extends beyond one year, then this agreement should be reviewed at that time. Confidentiality agreements are suitable for internal employees as well.

The safeguarding of custom software is another important issue in regard to the use of contractors. Large corporations often employ contrac-
tors to develop custom software. It should be made clear in the language of the purchase agreement, that the software is owned by the corporation. Contractors must not be allowed to leave the premises with the software. These issues must be documented in the contractual terms of agreement.

Information and systems should be classified according to their sensitivity and criticality. Proper procedures for handling classified information should be clearly defined, communicated, and made available to all employees.

NEED FOR INTERNAL CONTROLS

The organization’s first line of defense is an effective information protection program. To meet this need, effective internal controls must be implemented. These controls include procedures for adequate separation of duties for sensitive job functions or transactions and required vacation time or job rotation schedules. A surprising number of fraudulent occurrences are discovered when employees cannot report to work due to some unexpected event such as illness. In a recent case, a major financial institution uncovered a scheme that drained as much as $5 million through fraudulent wire-transfers. The breach was discovered only after a cashier, apparently one of the perpetrators, died suddenly.

Inadequate controls can lead to a poor return on stockholder investment, which can lead to stockholder anger, which can lead to charges of fiduciary negligence. As seen with some Fortune 100 companies recently, the stockholders have become militant in their demands to see that the directors and officers of the corporation manage their assets in a prudent and responsible manner.

Since the early 1990s, there has been an awakening with regard to the need for an effective corporate program of information protection. The new direction is that the program must be a corporate one rather than one based in the information systems organization. Many organizations have required each business unit to establish an information protection entity and charge that person with responsibility for ensuring that all employees were made aware of their individual responsibilities. An information protection program is part of the cost of doing business in the next millennium.

To be effective, it will be necessary to keep the information protection message visible to all employees. An effective awareness program examines the culture of an organization, the current level of compliance, and management expectations. The most effective way to ensure that a program will meet the organization’s business objectives is to understand what causes security programs to falter.
WHY DOES SECURITY FAIL?

Uncontrolled or Inadequately Controlled Access

The ability to control access to systems, data, and information is a vital element of any information protection program. Many times this first line of defense is breached and problems can occur. The following paragraphs describe how access control problems can affect an organization.

An employee working for a manufacturing facility in the Midwest was passed over for a promotion. Wanting to know who was better qualified than he was, he decided to access the human resources system. Once into the system, he found that employees were listed by job classification bands and then rated numerically based on their last appraisal. He felt that this was some valuable information, so he printed it out and then made enough copies so that he could post them on bulletin boards, the coffee machines, and in the cafeteria. The investigation turned up who was responsible for the postings and in his exit interview it was learned that he had gained access by using the director of HR's password. The HR director's password was still the default, new-user password — the first four characters of his last name.

A number of years ago, a Canadian software development firm was at an architecture convention and was showing its new computer-aided design package, an “expert system” for designing building facades. The owner and program developer were at one station and his son at a second station. After finishing a demonstration, the son turned his back on the computer for a few seconds. When he returned, a diskette was missing. Because they were updating the writer driver information, the diskette contained the source code. The estimated value of the software package was between $5–$10 million and represented 12 years of research and development.

In November 1988, Robert Morris, Jr., a graduate student in computer science at Cornell, wrote a self-replicating program called a worm and injected it into the Internet. The program was flawed and it began to replicate and reinfect machines at a much faster rate than he had anticipated. In 1988 there were almost 62,000 Internet host systems and it is estimated that Morris brought down about 10% of those systems. The estimated cost of dealing with the worm at each installation ranged from $200 to more than $53,000. Today there are nearly 20 million Internet host machines and a worm of the Morris magnitude could cause genuine havoc.

Vague or Inadequately Defined Responsibilities

Backups have always been a sticking point in the information systems environment. With the movement to distributed processing, the need for
users to perform and store backups has increased. Often times though, the users are not informed as to what their responsibilities are. If backups of a workstation are done at all, they are normally stored in the same area as the workstation and the same diskettes are reused. A large engineering firm was converting to PCs and employees were moving mainframe applications to their desktops. After about six months in the new processing environment, an office administrator called the help desk to request that her EXCEL spreadsheet be restored. The help desk directed her to the LAN administrator. The LAN administrator asked for her backup diskettes. She asked the LAN administrator about the backups that operations normally used to restore her old mainframe applications. Six months worth of conversion and updates were lost. Rules were changed and the customer was not informed.

A construction firm in Atlanta had what could be considered a rather lax backup and storage policy for diskettes. It seems that one weekend 50 diskettes disappeared from the offices. Of these 50 diskettes, 10 were considered to be crucially important. These 10 diskettes were so critical to the operation of the corporation, that if they were not found, the company faced the real possibility of going out of business. They were in the process of taking out an ad offering a reward in the Sunday papers, no questions asked. The ad never ran. The police found the diskettes. A maintenance employee had taken the diskettes home and was reformatting them so that his kids could play games on their new home computer. "People don’t leave out important diskettes, do they?” was his defense. By sheer luck, this company was able to avoid disaster.

A favorite group of people are drafting supervisors. They are a hardworking group and always seem to try to comply with company policies. One supervisor had just attended a workshop on the new database package. Being the conscientious person that he was, he decided to create a database to use what he had just learned. This database contained employees names, social security numbers, home addresses and phone numbers, current salary levels, and most recent appraisal information. He then attended a session on confidential information and wanted to ensure that the database was properly protected. Because he shared the workstation with the off-shift supervisors, he did not want to leave the database on the hard drive or a diskette in the shared desk. He decided to hide the diskette under the desk and attached it there with magnets. Sometimes one gets carried away with the desire to secure things.

Inadequate Training of Personnel
The software police (Business Software Alliance (BSA) and Software Publishers Association (SPA)) are continuing their effort to crack down on software piracy worldwide. In 1995, SPA increased its lawsuits and audits by 23% (586 organizations) and netted $2.6 million in penalties. Six
organizations reached settlements in excess of $100,000. Worldwide software piracy losses were estimated at $13.1 billion in 1995, an increase of 9% over the 1994 estimated losses.

Both BSA and SPA have 800 numbers that can be used for a number of reasons, including reporting possible copyright infringements. How do the software police find out about violations of copyright compliance? Initially, they received their information from employees who contacted the vendor for support. The vendor normally asks for the contact’s name, company name, and serial number. If different people are using the same software, then an investigation is started. Another way was that visitors, vendors, or contractors would observe the work habits of an organization and then turn them in for whatever reason. A third way was that disgruntled employees would turn in the company. Today, employees concerned about copyright compliance are calling the 800 numbers and giving information about their organization’s practices.

The computer virus problem is large and continues to grow. About 98% of all corporations and other large organizations have experienced computer virus infections. Since 1996, about 90% of all organizations with more than 500 PCs have experienced a computer virus encounter or incident each month. The chance of experiencing a computer virus incident is about one per 100 PCs per month. The cleanup cost per PC per year is more than $250. If the organization has 1,000 PCs or more, the virus-fighting costs can be estimated by taking the total number of PCs and multiplying by $250.

A Fortune 100 company discovered the Hi virus at a large division that was heavily networked with nine file servers and 630 client PCs. The site was also connected to 64 other sites around the world. The virus entered the division on a program disk from a legitimate European business partner. The virus was found one day after introduction and despite eradication efforts, it continued to infect the network for an entire month. The total cost of cleanup of the virus was $44,000, and does not include lost data.

With the advent of the information highway, many organizations have been faced with some form of abuse; these range from an employee accessing improper sites to the spreading of incorrect information. The Chaos Merchants are known to be anticommercial and antiestablishment hackers who steal the home pages of Web sites and leave a trademark picture of a naked woman, as they did when compromising Rodney Dangerfield’s Web site. With more than 18 million people a day accessing Web sites, hackers such as these could cause real problems for any organization.

The Government Accounting Office (GAO) reports that hackers infiltrate Pentagon computers more than 160,000 times per year. These attacks are rarely detected and seldom investigated. The Pentagon reports
that as many as 250,000 attempts may have been made to penetrate military computers in 1995, and that 65% (162,500) were successful.

An employee working for a media company in Philadelphia was using the company-provided Internet access an average of six hours per day to download pornography into his workstation, repackage it, and then sell it at computer fairs.

The use of electronic mail (E-mail) in business is spreading rapidly, and in many organizations the E-mail system is now the place for office gossip and other conversations unrelated to work. Although some of the exchanged information on E-mail is personal or frivolous, the system also frequently carries vital organization information. The “information mix” raises many moral and business issues that must be addressed.

In a recent Detroit Free Press article, two companies that were in litigation because of alleged discrimination lost their cases because of E-mail messages uncovered in the discovery process. In both instances, private communications between supervisors contained language that was used by the plaintiff’s attorney to support their client’s claims. In each case, the message could have been just an off-hand remark made between two colleagues. These remarks were costly both financially and to the company’s public image.

People do not use the same level of care when they are putting things into a computer. There is a false sense of privacy. When using the E-mail system, people tend to be more honest; it is where they are joking, and where they use their creativity. E-mail correspondence is as private as a postcard.

A Manhattan health company was using a new technology that allows users to tape themselves with a tiny camera built into the monitor of their workstation and send a moving image message through the system. A high-level executive decided to use the system one night from her hotel room. Sitting in front of her notebook in the privacy of her hotel room, she purred to the intended recipient, a fellow married colleague, “Hurry to the hotel and here’s what you get tonight.” With that, she did what has been described as a “strip shimmy.” Then, instead of sending the message out as private, she inadvertently used the public feature and sent the message to more than 400 employees.

All too often, employees fail to understand the need to protect classified information. When working through the courts to determine if information is in fact trade secret, the courts look for four keys:

1. that there was some cost to develop this product or process;
2. that the product or process will provide some form of competitive advantage;
3. that the product or process is not generally known; and
4. the information is kept secret both externally and internally.
Where most organizations fail is in the need to keep the information secret both externally and internally. Many employees fax sensitive information in clear text or will discuss such information over cellular or wireless phones. When this behavior occurs, the information is no longer confidential, but becomes public domain.

Employees’ Exposure to Unnecessary Temptation

Many of the examples in this category fall under the heading of separation of duties or rotation of assignments. All too often employees are able to stay in a job assignment long enough to determine what would trigger an audit or review. One such individual was an analyst working for the Federal government. This individual was responsible for reviewing expense reports and then submitting them directly to disbursement for payment. No one checked his work. In fact, no one questioned any of his activities until a mortgage processor could not make his assets match his earnings. This individual was purchasing a $350,000 home in the Washington, D.C. area (paying for almost all of it in cash), had several very expensive automobiles, country club memberships, and original oil paintings, and was remarried with two children. He was able to afford all of this on a salary of $40,000 per year and paying $1,000 a month in child support.

It seems that he found out that many departments were not using all of their travel and expense money. With what little was left over, it seemed a shame to turn it back into the government. So he began to create expense reports to himself. Over an 18-month period, he wrote checks to the tune of $1.2 million. The Federal government admits that if it had not been for the mortgage processor, they might never have uncovered his scheme.

The company E-mail system is often an avenue for abuse. An Air Force Master Sergeant was convicted of misuse of a government computer; distribution of obscene writing; communicating indecent language on sexual topics; and obstruction of justice for allegedly trying to delete his E-mail.

On many systems, it is easy to send an E-mail message that appears to come from someone other than the actual sender. At a university in New England, a student spoofed an E-mail message from the department secretary, canceling an exam. Half the students did not show up. At a university in the Midwest, someone forged a letter of resignation from the director of housing to the chancellor. A New England housewife discovered that a Chicago man was sending obscene messages in her name.

When it comes to the loss of company secrets, one of the most dangerous and hardest to spot is the trusted employee. The most likely candidates are employees who may be disgruntled, or have incurred large
debts due to gambling habits, personal circumstances, or drug use. According to Insights, 10% of workers are abusing drugs and/or alcohol on the job. Other reasons include involvement with labor-management disputes or having entrepreneurial personalities. The typical computer criminal is a nontechnical user of the system or application who has been around long enough to figure out what would cause an audit.

An electrical supply company in Nebraska had an employee who was responsible for paying the invoices and reconciling the company checking account. Her scheme was not high-tech; she would receive an invoice, write the check for the proper amount, but would enter a higher amount in the check register and then write out a check to herself for the difference. In the register for the second check she would write void. When the bank statement would come, she would destroy the check to herself and then balance out the account. In three years, she managed to take $450,000. She became remorseful and turned herself in to the authorities.

Another area of employee temptation is the theft of notebook computers. A recent Wall Street Journal article indicated that over 200,000 notebook computers are reported stolen each year and less than 10% are ever recovered. The most significant of these losses was during Operation Desert Storm. A NATO officer had his laptop stolen from his car. The computer contained all of the command codes for the operation.

Inadequate Protection against Disgruntled Employees

An employee working for a large manufacturing corporation had a unique solution to a password problem. One Monday morning, after incorrectly entering his password four times and having his access revoked, the employee called the Help Desk to inform them that his computer did not work. After verifying who he was, the Help Desk operator reset his password and told him to try again. The employee repeated his problem: "My computer does not work." After vainly attempting to walk the employee through the process, she decided to call for level 2 support and have them meet with the employee to see what the problem was. After revoking his access, the employee went to his locker and got out a .38 Police Special and fired one round into the CRT. He was right, his computer did not work.

Another employee was let go by a firm but was given a two-week notice. He was their LAN administrator and felt that he was being treated unfairly during the corporate downsizing. To make things more lively after he left, he decided to put a 4MB cap on the system directory. Three months after he left, the office came to a halt until the problem could be found and corrected.

The Business Software Alliance (BSA) and Software Publishers Association (SPA) have installed hotlines that supply information on copyright
compliance. Last year BSA received 7,000 calls on its hotline; about half of them were employees who wanted to rat on companies who were using unlicensed software. Of these complaints, nearly 500 resulted in cases with recoveries reaching almost $4 million.

Passwords (Failing to Meet the Challenges of the 21st Century)
The most cost-effective form of access control is still the use of reusable passwords. However, as long as there are employees using these confidential access codes, there will be problems. When conducting an initial security review, looking for passwords is no more difficult than turning over a keyboard, opening an unlocked middle desk drawer, flipping to "P" in a Rolodex, or looking for a note posted to the CRT.

When Commonwealth Films, Inc., was shooting the video Mum's The Word, the director was setting a scene that showed an employee's password taped to the side of the terminal. The technical advisor was concerned that what was being shown was outdated. The company where the video was being made had an extensive employee awareness program that stressed password security. Leaning into the cube across from the video setup, the technical advisor asked, "If you were going to post your password, where would you do it?" The woman pointed to a note on her workstation and said, "Mine's right there." Her rationale was that people would need to know how to access the system in order to use her password.

The Internet has experienced some incidents dealing with password sniffing. Password sniffer programs monitor the system's network interface port and collect login information, including passwords. The program is put into the system after the attacker has obtained privileged status on a target host system. This is done by exploiting any of a number of known attack methods. This can normally only happen when the host system has not been properly configured and administered to prevent unauthorized access.

A major problem for every organization is the current status of all individuals who have been granted access. Employees, contractors, vendors, suppliers, and customers have been granted access to the system over the years. The hard part is having someone contact account administration with the same level of urgency when access is to be removed. An automotive company was receiving a monthly bill for $350,000 in usage and storage charges for 688 users of an outside engineering service. During a reorganization, the cost of the service came under question. Over half of the accounts had not been used in 18 months and the remaining accounts lacked contact information. It took two months to sort out all of the account information, and the end result was a reduction in monthly fees and user accounts by nearly 80%.
Exposure of Sensitive Information in the Trash

Stealing garbage is easier than most people think and it also provides a wealth of information. Most trash bins are placed within easy public access and the good spy will always dip in. All one has to do is go through the plastic garbage bags, checking envelopes and the like to ascertain who the garbage belongs to. The garbage can then be removed to a safer place for more in-depth examination. This operation can be conducted on a regular basis with startling results. The Supreme Court has ruled that the Fourth Amendment does not prohibit the search of garbage placed outside the premises. It is legal! Many private investigators now openly advertise garbage retrieval services.

The owner of a bottled gas company in the Midwest boasted to friends and colleagues that he “rooted around like a pig” in his competitor's dumpster and was able to get their customer lists.

Trash is valuable; all waste paper should be destroyed. Shredders should be purchased to meet the needs of all employees, both at work and away. A chief financial officer for a Fortune 100 company contacted the security staff and informed them that his trash was picked up on Thursday evening. The security staff replied that he probably had a clean yard for the weekend. The CFO then added that the rest of the neighborhood had their trash picked up on Friday morning. His work habits were well known — he normally took home two transfer cases of papers to be worked on each evening. The company quickly purchased a shredder for home use.

Many of the teens who have gone on to bigger and better things got their start by doing some dumpster diving. Kevin Mitnick and his group were able to begin their work by accessing the trash at a number of locations. There are many other such “celebrities” who have gained access to banks, telephone companies, utilities, and other companies. The 2600 magazine (the quarterly guide for the American hacker) ran an article on how to become a member of a contract cleaning crew and described how to gain access to company information.

WE ARE OUR OWN WORST ENEMIES

For the most part, management will suffer self-inflicted information protection problems. A policy on copyright compliance may be established and then turned away when employees try to “save” the company money by “evaluating” software at the office. How can an organization have an effective information protection policy when federal copyright law is ignored? The employees follow the lead set by management. If the policies are established and followed by management, then the employees will do the same. However, if they see that management selects the policies that they feel are worth following, then the employees will be able to rationalize why they do not have to follow certain policies.
Another example of these self-inflicted problems is the introduction of computer viruses into the workplace. Many companies will spend large amounts of money to deploy an anti-virus package across the network, only to have the employees turn them off because the product slows down the boot-up process. Or the company encourages employees to work at home, but fails to provide either an anti-virus product for the home system or does not have virus scanning stations around the office.

The biggest problem area is the sharing of passwords. Since at least 1974 (the founding of the computer security industry), password abuse has been the number-one problem in computer and information security. Although everyone in the industry is aware of the shortcomings of passwords, they are still the most cost-effective first lines of defense. Employees need to be reminded regularly of their responsibilities regarding passwords protection: for example, choosing the proper password, not leaving it lying around, and changing it on a regular basis.

RESOLVING THE DILEMMA

Attain Senior Management Approval and Support

Security issues must be tied to business objectives and/or the mission statement. Implementing controls to be in compliance with audit requirements is not the reason to do anything. In order to sell an effective program and get the buy-in from senior management, it will be necessary to identify to them how this process will support the organization’s mission. Every organization has a bottom line; therefore, security issues should always be discussed with regards to how they will support that goal.

Stress the benefits of an effective program. Learn the needs of the different organizations and make certain that the sales pitch addresses their concerns. Be prepared to identify the costs of having an inadequate program, the loss of customer confidence, competitive advantage, and business.

Establish Enterprisewide Policies

The key to any successful program is to have published policies. The policies must also meet the needs and the culture of the enterprise. To be successful, the policies must meet the needs of the customers. Find out what concerns the user community has, and structure the policies to meet those needs. When developing policies, remember to keep things simple. The reading and comprehension level of most employees is that of a sixth grader: Keep the information short and to the point.

Implement an Enterprisewide Awareness Program

It is vitally necessary to keep the security message in front of the employees. It is not sufficient to publish policies. Employees must be made
aware of their existence and this must be done on at least an annual basis. To complete this process, it will be necessary to develop a method of getting the information to contract personnel. It may not be possible or desirable to include contract personnel in employee training. Because of the legal implications, contract personnel must be informed, but this must be done through contract negotiation with the contract house.

Monitor Compliance
Whenever a new security project is about to begin, it is recommended that the staff takes an evening or two to do a walkabout. They should walk through the office environment and check to see the current level of compliance to some very minor security controls. During this initial review, five key elements should be checked:

- offices are locked
- desks and file cabinets are locked
- workstations are secured
- diskettes are secured
- information is secured

These five controls will provide a good indication of the current level of concern over computer and information security. Normally, the noncompliance levels during this initial review will be 90% and higher. This information can be used to gauge the information protection program’s effectiveness by doing another walkabout after the program has been rolled out.

Another key element in monitoring compliance is to establish a positive working relationship with the audit staff. If the audit staff is visible only when they are in doing an audit, then the working relationship is probably weak. Audit and information protection are working the same issues for the company. It would be beneficial for all involved to work together to prepare a consolidated front in getting security controls accepted.

Make Compliance an Appraisal Item
Most employees are required to read and sign an annual Conflict of Interest Statement. Work with the audit staff to create an Employee Rights and Responsibilities for Information Access statement. This document could be included with the Conflict of Interest Statement and reviewed annually with the employees.

For senior level management, it may be necessary to create an Employment Agreement. This agreement is used by many companies for senior level executives and certain employees who have access to highly confidential and proprietary information. Such agreements restrict employment with a competitor for a period of time after leaving the compa-
ny. This is a very complicated legal document and will require research and coordination with the human resources and legal staffs.

SECURITY AS PART OF THE ENTERPRISE INFRASTRUCTURE

The objective of any information protection program is to provide acceptable business controls. The goal is to ensure that senior management meets its fiduciary responsibilities with regard to protecting the information assets of the enterprise. For many organizations, it comes as a surprise that information is an asset and is the property of the enterprise. As such, it requires that specific controls are in place to ensure that it is properly protected from unauthorized access, modification, destruction, and disclosure.

An effective program will also enhance employee and workplace efficiencies. By putting a business-directed program in place, access to information will become structured. Employees will learn the process and will be able to gain the resources they need in a timely and efficient manner. Additionally, by having business-related controls in place, efforts and resources are not wasted on protecting information that does not require it.

By restricting access to the logical and physical assets of an organization, the possibility for theft will be reduced. This does not mean that theft will be eliminated. There will always be some loss due to employee or outsider theft. The goal of an effective program is to reduce the theft to an acceptable level. Management at a chicken processing plant in North Carolina believed that its employees were stealing some of their chickens. To prevent the employees from stealing, the management decided to lock all but the main exit. However, when a fire broke out and the employees attempted to leave through the fire exits, they found that they had been padlocked. Over 25 employees died because of this decision. Remember that the goal of any protection program is to reduce risk to an acceptable level. Putting employee lives in jeopardy is not an acceptable level of control.

SUMMARY

Just as steps have been taken to protect employees, it is now necessary to involve the employees in protecting the information assets. Information must be protected from unauthorized access, modification, destruction, and disclosure. If the enterprise fails to do this, there will be a loss of customer confidence, competitive advantage, and ultimately, jobs. Information protection is not rocket science or nuclear physics. It is taking basic business principles and applying them to the information assets of the enterprise.

The message of information protection must be first published, and then presented to the employees through an effective awareness pro-
gram. This program must include regular reminders regarding protection of enterprise assets and responsibility for protecting those assets.

Once the program is in effect, employees at all levels of the organization will learn that they are responsible for protecting the information and computer resources of the enterprise.

Tom Peliter is a senior security consultant with CyberSafe, Inc.