EDP ANALYZER

© 1979 by Canning Publications, Inc.

JULY, 1979
VOL. 17, NO. 7

THE SECURITY OF MANAGERS' INFORMATION

Security measures are needed to protect against the unauthorized modification, destruction, or disclosure of computerized records—such as customer account records, employee payroll records, etc. But today's data security measures are not fully effective. We have been told that just about *every* carefully planned penetration effort, made to test the security of a system, has been successful. With the advent of the automated office, the problem will be intensified. Management's letters, memos, tickler files, travel plans, and so on will be in computer files and will be just as available to penetrators as are today's data files. Here are some suggestions on steps you can take to determine security requirements for automated office systems.

At a talk given in Los Angeles last fall, Robert L. Patrick of Northridge, California, a pioneer computer consultant, said, "I have performed a lot of audits of computer centers, ranging in size from several small mini-computers to a network of IBM 370/168s. There is one problem that has shown up in these audits time and time again, and that is *a lack of security.*"

His involvement with computer security began in the early 1970s, said Patrick, when he was asked to author the first AFIPS Best Practices manual on security (Reference 1). This first edition of the manual was published in 1974. It was a huge checklist for making a security audit, containing over 800 questions. With this background, Patrick soon found himself looking carefully at security measures while he was performing management audits of computer installations.

One of his experiences illustrates the vulnerabilities that exist in most office environments. In this instance, Patrick was making a management audit at a company. Company executives felt that their office security measures were probably adequate but asked him to check those measures, as a part of his audit.

So Patrick showed up one evening while the janitors were busy in the building. Security may be great during the day—but janitors often unlock a lot of doors when they are on the premises to clean the offices. So it was not too difficult for him to get in.

He then made his way to the offices of key executives, taking care not to be seen by the janitors. Upon reaching an office, he would try the door to the office and, often as not, find it locked. He then looked in the secretary's desk for keys. Secretaries usually have keys to their bosses' offices, but they hide the keys on the premises rather than carry them. The typical hiding places are in their desks, or in small card file boxes on their desks, or in their filing cabinets. Further, the secretaries have found that they must cover for each other; if a secretary is sick, another secretary must know where the keys are. So, if the keys to a boss' office and desk were locked in the secretary's desk, Patrick could find a key to that desk in another nearby secretary's desk, in most cases.

It thus proved to be fairly easy for him to gain access to the *desk drawers* of the executives he had singled out. Having gained access, he left his business card in plain sight in each desk, locked up the drawers and the offices, and returned the keys to where he had found them.

In addition, this company had a 'strong room' in which the most sensitive financial data, charts, and records were kept. Only the controller had the key to the strong room—but the controller, treasurer, and director of finance all covered for each other, in case one was sick or on a trip. In a secretary's desk, Patrick found the key to the treasurer's office, where he found the key to the director of finance's office, where he found the key to the controller's office, where he found the key to the strong room. So he stretched a piece of tape across the interior of the strong room and stuck his card to it.

But the penetration did not end there. The company had a control center on the top floor of a high rise portion of the building. Not only were there a lot of the critical controls located in this center but also there were fire alarm switches, other alarm switches, and television monitors for watching important doors and corridors. And there was a locked key cabinet in which were stored the keys for entering all parts of the building. In theory, the control center was well protected; in actuality, it was vulnerable. Access could be gained either by stairs or by a freight elevator—and the elevator had a floor indicator dial at each floor. During the night-time hours, when only a skeleton crew was on duty, if the elevator was not at the top floor, then Patrick knew that the control center probably was vacant at that time, since only one person was on duty. So he waited until the elevator moved to an intermediate floor, and then went up the stairs and into the control center. There he found a cutting torch with which he could have opened the key cabinet. He taped his business card to the key cabinet and then left. And went back to his hotel.

The next morning, he came in early at about 7:30, and went to the company cafeteria to get coffee. In the coffee line, he met the general manager who said to him, "I hear you left some calling cards last night. Did you leave one for me?" "No," said Patrick, "I couldn't get into your office." It was clear that the penetration had been discovered very early and that the general manager and others had been called as soon as it had been discovered.

In another audit, a vault was used in the computer room for storing tapes, check forms, check signature imprinter, and so on. The walls and flooring were reinforced and a very strong door was used. But these vault walls did not extend all of the way to the true ceiling of the room but rather only to above the false ceiling. So, said Patrick, anyone with a few hours of time could easily penetrate the vault by cutting through above the reinforced wall.

Patrick concluded his talk, to a group of computer professionals, with the statement, "Your company assets are probably not as secure as you think they are, especially if they exist in your computer center."

Electronic access

The above experience illustrates how a shrewd penetrator might gain physical access to a company's offices, control center, and computer center. But it is just as possible, if not more so, for a penetrator to gain access to computerized files via a remote terminal.

Early this year, newspapers carried the story of how a 15-year old boy in California used second-hand equipment that he had bought for $60 to dial in to the University of California's computer center. And when he did get into the computer, he did mischief—material was missing, material was added, etc.

Computer center authorities soon identified the penetrator and warned him to stop—and spent night and weekend hours cleaning up any damage and bolstering the security measures with violation traps. The boy presumably detected these, because a message was found in the system, "You've done relatively well keeping me out; would you like some help?"

The university finally found it necessary to charge the boy with (1) grand theft, for stealing more than 200 hours of computer time, with (2) felony vandalism, for disrupting the university computer system, and with (3) possession of stolen property, the printouts he had made of other people's work.

As the newspaper article said, the boy was not old enough to obtain a driver's license—but he was old enough and smart enough to penetrate the computer system. Representatives of the university made the point that the boy had been given instruction on the use of the system, as a part of a high school indoctrination program, and that the system had been made 'friendly,' for ease of use by non-professionals. Computer security was considered adequate to prevent accidental misuse and to deter most intentional misuse. But such safeguards can be bypassed, and the boy managed to do it.

These, then, are two examples of unauthorized access to data and information. The first involved physical access and the second was access via a remote terminal. Note that the easy-to-use, friendly user interface for the university system is just what system designers will attempt to provide with on-line computer services for managers. Almost any organization can (and should) see itself as the target of such penetrations. All that is needed is that a shrewd penetrator have a desire, rational or irrational, to make the penetration.

The changing environment

Why should organizations be more concerned about security than has perhaps been true in the past? For one thing, the business and social environment is becoming less benign. Some elements of society see nothing wrong in stealing from companies. Others want to obtain embarrassing information from company files in order to pressure a company into a course of action they support.

In other instances, the only change in the environment is the relative ease of penetration. Competitive firms, for instance, might hesitate to physically penetrate a company's premises and files but have no hesitation in gaining access to computerized files from a remote terminal.

Within a company, there well may be cases of unauthorized access to data and information. Competition among managers, each seeking promotion, may lead them to look for 'interesting' material in the files of other managers.

The subject of *data* security has received a good amount of attention, and management in general is aware of the problems. True, the attitude that "it can't happen to us" too often exists—until a penetration is discovered. But at least the problem is recognized.

In the area of the newly-emerging automated office, we suspect that the problem of *information* security is not yet widely recognized. The automated office is still so new that most of the attention is directed toward the benefits and the problems of installing this new technology. The threats and vulnerabilities may not yet have been considered.

But a little thought will make it clear that the penetration methods used for getting at data can be just as easily used to get at information in automated office files. In fact, the payoff for the penetrator may be much greater, if management information is obtained.

Many organizations still have inadequate security measures for their data processing, it would appear; witness Patrick's general comment based on his audits. Not only is it important for such organizations to bolster their data processing security, if they are moving toward the automated office the need for security becomes almost imperative.

Last month, we discussed two approaches for determining managers' requirements for information. In this report, we will consider how to determine the security requirements for that information. To begin the discussion, here are some definitions of key terms.

Definition of terms

Various authors writing on the subject of security have used a number of key terms in an inconsistent manner. Apparently there are no standard definitions in the field, as yet. These terms include: threats, risks, vulnerabilities, exposures, and so on. Following is the way we will use them.

Threats. While dictionaries define a threat as "an indication of an impending danger; a message or warning of a harm or loss," most usage in the security context applies to the *danger itself*, not the warning. So a list of threats means a list of dangers to which a person, an organization, and/or a system can be exposed.

Vulnerabilities. Given a threat (danger), a vulnerability is a lack of protection against that threat. It is the susceptibility of the person, organization, or system to harm from that threat.

Risks. The risk is the likelihood (chance) that the danger will come to pass. Ultimately, it is determined by subjective judgment. To aid that judgment, statistics based on the experiences of others may be available.

Exposure. If the danger does, in fact, come to pass against a vulnerable person, organization, or system, the exposure is the harm or loss that can result—the consequences. The bad consequences, of course, are what the security measures are designed to prevent.

Expected loss. This is defined as the exposure multiplied by the risk. In concept, it is somewhat like an insurance premium which is paid every year in order to cover a loss when it does occur. We will discuss this concept in more detail below.

Vulnerability analysis. Given a specific danger, a vulnerability analysis seeks to determine the degree of protection that exists against that danger and the consequences (to the person, organization, or system) that can result if the danger materializes.

Risk analysis. Given a list of specific dangers, what are the likelihoods that the dangers will actually come to pass. For example, an earthquake can conceivably occur anywhere on earth, but the risk of an earthquake is higher in California than it is in, say, Kansas.

Vulnerability/risk analysis. The results of this analysis really are 'the bottom line' for security planning. For each specific danger, it indicates the likelihood of that danger happening and the harm or loss that will result from it happening. In the worst case, the organization may be forced out business. In many other instances of danger, the harm will be more of an annoyance. The vulnerability/risk analysis attempts to rank the dangers, in terms of how likely they are to occur and what can happen if they do occur.

Let us now look at some studies concerning computer misuse in the data processing field, to indicate types of security problems to be considered for the automated office.

Threats to data processing

Studies of detected computer misuse to date have shown that a large percentage of the cases are fraud and embezzlement cases. The perpetrators have a new tool, the computer, and the amounts of money involved generally are larger than has been true in manual systems—but the objectives are the same. Then there has been some theft of data, perhaps for the purpose of selling to third parties. The remainder of the cases have mainly involved destruction of data or equipment or the denial of computer services to legitimate users.

Chambers (Reference 2) and Jacobson (Reference 3) have made analyses of detected computer misuse that was reported by others. Donn Parker of SRI International has been the source of many of the reported figures.

Chambers points out that the objective of most of the computer misuse has been to influence system output—delay it, prevent its preparation, damage it, destroy it, use it, alter it, copy it, steal it, or some combination of these.

In a study of 33 cases of detected misuse, Chambers found that members of the computer staff itself (analysts, programmers, operators) were the perpetrators 42% of the time, while outsiders (to the company) were the offenders 33% of the time, and users (within the company) constituted the remaining 25% of the cases.

The point of attack of these perpetrators was: manipulation of input (45% of the cases), hands-on use or damage of the computer itself (27%), modification of computer programs (24%), and other (4%). The manipulation of input was used by all three groups of perpetrators; the hands-on use or damage of the computer itself was performed mainly by outsiders;

and the modification of computer programs was done almost entirely by the computer staff.

Jacobson believes that the great majority of computer crime cases are *not* published, and that those which are published are not representative. He points out that relatively too much attention may be paid to the 'big four' types of computer misuse—inserting false input data, stealing master file data, stealing computer services, and damage or destruction of computer equipment. There are seven other types of misuse that may be relatively understated, and by a significant amount, he feels. They may (and probably do, he says) occur much more frequently than the statistics indicate. But when they are detected, the organizations involved tend to keep quiet about them, so they never show up in the statistics.

These other types of misuse, says Jacobson, include the suppression, alteration, or theft of output, alteration or damage of master files, and the modification of programs.

Statistics on computer misuse can be helpful, in that they indicate potential dangers, based on the experiences of others. But it should also be recognized, as Jacobson points out, that there are reasons why the statistics are incomplete and why they may well be giving biased views on the dangers.

Then there is another factor to consider—the change in the data processing environment.

A variety of environments. The U.S. National Bureau of Standards and the General Accounting Office jointly sponsored a workshop in early 1977 on the subject of "the audit and evaluation of computer security," which is documented in Reference 4a. One of the workshop panels presented the following taxonomy of system environments.

Five main parameters were presented for defining a system environment. *Type of service* refers to either batch or interactive service; real-time control applications were considered outside the scope of the discussion. The *organization* of the system can be either centralized or decentralized. The *user access* may be either local or remote. The *application software* can be either dedicated or multi-purpose. And the *degree of sharing* is either single user or multiple users.

During the 1960s and early 1970s, when many of the published cases of computer misuse occurred, the typical computer environment was the following: batch, centralized, local access only, dedicated application software, but multiple users of the central facility. This environment was sure to influence the statistics that have been reported. For instance, 27% of the cases analyzed by Chambers involved the perpetrator either getting hands-on access to the computer or physically damaging the computer, by bomb or fire or such. Also, files were often copied or erased by means of this hands-on access. Physical access was necessary for performing such misuses on strictly local batch systems.

With the spread of interactive systems that use remote terminals, the statistics of misuse probably will change. While some physical access will occur, there will be a growth of unauthorized access from remote terminals. So files can be copied, modified, or damaged from remote locations. Also, the physical destruction of the equipment might well diminish, but the theft of terminals and micro-computers probably will increase.

So, while the types of threats to data processing systems may remain about the same, the relative frequency with which each type of threat occurs probably will change. The statistics of the past, imperfect as they were, will probably deviate further and further from the current situation.

In summary, most of the detected cases of computer misuse in data processing have involved batch-type central systems. The misuse involved (a) the manipulation of input, generally to get a desired output, (b) the modification of computer programs, generally to get a desired illicit output or to suppress a legitimate output, (c) the physical theft of output documents, (d) the physical theft of master files, and (e) the alteration or damage of master files.

In the new on-line data processing environment, the threats will shift (relatively) from physical access, theft, or damage to electronic access and the copying of information in electronic files, we suspect.

And note that this new data processing environment is essentially the same as that proposed for the automated office. So the types of threats to information in managers' electronic files will be very similar to those for on-line data files.

But, in addition, the automated office may have some threats of its own.

Threats to the automated office

Because the automated office is still in its initial stages, not much is known about the types and relative frequency of threats. We believe that that the types of threats known to have materialized for data processing will also be likely for the automated office. But there well may be some differences.

One possible difference that we see is the following. As mentioned earlier, the threats to data processing are largely the familiar fraud and embezzlement crimes, where the perpetrators seek to divert negotiable instruments to their own uses. With the automated office, we believe that the misuses are more likely to resemble industrial espionage. The perpetrators will seek access to information in the managers' files in order to learn about plans, or to influence plans or actions by modifying or destroying information. And all of that information may be readily available to the penetrator.

Let us briefly review what the automated office environment will be like (as we have discussed in our September and October 1978, and May and June 1979, reports).

The environment. We see the automated office as eventually consisting of a large number of terminals or work-stations, which can perform work in a stand-alone manner and which can also be tied into one or more data communications networks. Secretaries will use work-stations instead of typewriters. Managers and staff members will use work-stations in addition to their telephones.

Components. A typical work-station will consist of a CRT terminal, perhaps a hard-copy printer, a micro-computer, one or more floppy disk drives, a data communications interface, and a modem. The work-station will be able to perform all of the functions needed for maintaining local files, stored on floppy disks. It will also be able to communicate with other work-stations, as well as with corporate data services, by way of the data communications network. And it will be able to access computer services offered via public networks.

Each computer-using organization may well have a central system that performs a message switching function among the work-stations, and that has central indexes to information files.

Functions. We see the work-stations as being able to perform (1) word processing functions, (2) receiving and sending messages by way of the computer message system, (3) storing the user's personal files, and (4) providing the user's personal decision support functions. The personal files can include: outgoing correspondence, both incoming and outgoing intra-company messages, daily calendar, appointment schedule, travel plans, tickler file, work assignment file, and so on.

In short, much of what is now recorded and stored on paper, and some of what is transmitted over the telephone and by informal meetings, will be handled electronically.

In such an environment, what might be some of the threats?

The possible threats. As mentioned above, we see misuse of the information files in the automated office as being more like industrial espionage and less like fraud and embezzlement. The reason is that the managers' personal files do not provide access to negotiable instruments the way data processing records do. Penetrators will probably seek to copy files more than they will seek to influence normal outputs.

Physical access to the work-stations of managers and secretaries will be a significant threat, we suspect. It would seem that most work-stations may not be connected to the data communications network at all times but rather only when the user so desires the connection. Hence, access to a work-stations files from a remote terminal would be possible only when that work-station is connected on-line.

It would be quite possible for a penetrator to gain access to offices in ways such as those discussed at the beginning of this report. Having gained access, he or she could use the work-station to copy files onto blank floppy disks, to learn passwords for accessing sensitive files on the central system (copied down by secretaries and stored in their desks, as they do with office and desk keys), or to destroy the files and all backup copies of files that could be found.

Remote access to the work-station's files will be possible when the work-station is connected to the network and the files are on-line. As is true with any on-line files, the penetrator may be able to read those files, modify them, destroy parts or all of some files, insert fraudulent records, and insert program bugs.

It seems to us that the dangers are real ones. They are all well within the state of the art for penetrators. The questions then become: how likely is it that these dangers will come to pass and, if they do, what will be the consequences?

Defining the problem

The above discussion has dealt mainly with threats and dangers. But for any particular organization, there are several other factors that must be considered for defining the security problem.

Vulnerabilities must be considered—that is, the weakness or lack of protection in the organization that exist against specific threats.

Consequences to the organization (the exposure), if one or more of those threats actually come to pass, must also be considered. And finally,

Risks must be assessed—that is, the likelihood that the threats will occur.

How might an organization approach the definition of its security problem? We see two main steps involved in getting started:

- Obtain management support
- Select top-down or bottom-up

We will discuss each of these points.

Management support

On the basis of the above discussion, pointing out the relative ease with which penetrations may be made, it might be assumed that "of course management will support a program to provide adequate security." But this assumption is not necessarily valid.

For one thing, most managers are innundated with immediate problems. The one thing they feel they do *not* need is to be further burdened with hypothetical problems. But security deals with hypothetical problems—things that *might* happen.

Further, these are things that management hopes will never happen. And they involve 'bad' human behavior, in most cases, while managers prefer to deal with 'good' behavior,—such as: how employees can get their work done, get company problems solved, and so on.

The net result, as one might expect, is that security considerations tend to be postponed. They are postponed, that is, until some serious consequence occurs from a breach of security. Then there may be a flurry of excitement, as an attempt is made to bolster security measures.

As we see it, management's willingness to consider the security problem is the most important single factor in the whole security program. We hope that the reason for this belief will become apparent in the discussion that follows.

For one thing, a rather critical decision must be made at the outset. That decision is whether the security problem should be approached on a top-down basis or on a bottom-up basis; we will have more to say about those two approaches shortly.

Executive management's active participation is needed on several other points, also. For one thing, management must set the policies, ground rules, and scope of the security project. Further, management must be willing to hold periodic reviews of the subject, to see whether things have changed to the point where major new protective measures must be considered. And in the interim between these periodic reviews, there must be a willingness to attend to trouble reports, suggestions, etc., that are brought up by the people charged with the security program.

But top management is already swamped, some may say; is it realistic to ask them to be concerned with this problem area? Cannot executive management just delegate the responsibility?

Well, as we will point out in the discussion of the top-down approach, the security problem really begins with a consideration of threats that can *literally destroy* an organization and we cite examples of types of organizations that have rather recently undergone this experience. Surely nothing is more deserving of top management's attention than things that threaten the very existence of the organization. If this seems rather extreme and implausible, read on.

To begin, though, let us first consider the bottom-up approach. This is the more conventional approach to the security problem, we suspect, and the one that most organizations will tend to adopt.

Bottom-up approach

We use the term 'bottom-up' because the approach to be described here gets into the selection of control techniques very quickly. The threats that the organization faces are considered to be well-known, and the control techniques that can be used are also well-known. So the program consists, in the main, of (a) using certain basic types of controls that it is felt all organizations should use, and (b) then selecting and using certain other controls to meet the needs of the specific situation.

We do not wish to imply a criticism of this approach by the use of the term 'bottom-up.' It is a valid approach and, as mentioned, is one that many organizations will prefer to use. And we also don't want to imply that there is anything 'standard' about the approach. The discussion that follows is simply one way of going about it. We have participated in a number of workshop sessions on this general subject and each session has approached the subject in a somewhat different manner.

One publication that we believe will reflect the viewpoint of this approach is Reference 4b. Our discussion draws upon the workshop which will be reported in that publication.

Another name that might be given to this approach is "every organization needs an effective system of internal controls." The approach deals with the handling of assets and liabilities of an organization, and primarily with the current assets and liabilities. Examples of those things to which internal controls are applied include cash, cash equivalents, accounts receivable, accounts payable, inventory, payroll, and so on.

The main point here is that every organization has a well-recognized set of assets and liabilities that need to be protected. No big study is needed to determine their existence, importance, or need for protection. Further, these assets and liabilities can be protected, in part, by protecting information about them. If a fictitious payment transaction is entered into the accounts receivable file, an asset is lost. Also, if a fictitious invoice is entered into the accounts payable file and is paid, an asset is lost. Protection against these threats is accomplished by controls that make it difficult to enter such fictitious transactions.

So, say the adherents of this approach, computer security can be provided by the use of an effective system of internal controls. Nothing fundamentally new is involved.

Overall program

What is needed in the bottom-up approach is a program consisting of the following parts.

Management support for the program, in the form of (1) assignment of major responsibilities for the program, (2) organization and assignment of team members, and (3) setting policies and general control objectives.

For instance, the American Institute of Certified Public Accountants has published a set of general control standards, Reference 5. One such general control standard can be stated as, "There should be a separtion of functions between the EDP department and the users." Another is, "There should be a segregation of duties *within* the EDP department." Management can set the desired tone for the whole security program by identifying those general control standards that it wishes to emphasize.

Study of existing controls, to point out where additional or improved controls are needed.

Design and install the needed controls, under the responsibility of operating management.

Finally, *check the effectiveness* of the whole internal control system by means of periodic audits.

Of course, more must be said about the second step—that of studying the existing controls and pointing out where additional or improved controls are needed. Which leads into the subject of control objectives.

Control objectives. Control objectives seek to answer the question: what should be accomplished by the internal control system? What is to be protected and, in general, how?

As we understand it, control objectives are set by first identifying the potential targets of threats—that is, the current assets, liabilities, sensitive information, critical equipment, and so on. Then the flow of information is determined that pertains to these targets. Next, the actions that are *desired* relative to these targets are specified; an example would be the posting of a legitimate payment to an open account in the accounts receivable file. These are the actions that are to be allowed to occur by the internal control system. Finally, the types of actions that are *not desired*, and thus should not be allowed, must be identified. Controls are needed for detecting and (hopefully) preventing these undesirable actions.

Exposure analysis. In the bottom-up approach, we gather that a risk analysis generally is not attempted. One reason is that this type of analysis is considered too subjective. Rather, it is assumed that if a threat can occur, it must be protected against—subject, of course, to "the use of common sense."

So, instead of a risk analysis, an exposure analysis is performed. This analysis addresses the question: what possible damage can occur to the organization if a particular type of threat materializes? The current conrols are then evaluated in light of these exposures, to determine what additional controls might be needed.

The end result of the bottom-up analysis, then, is a list of threat/control pairs. For each type of threat, one or more types of controls are proposed for detecting and possibly preventing the threat from doing damage. Some controls are considered primary and other secondary. It is then up to management to decide which controls will be used.

Some observations

With this bottom-up approach, the control system designers get into the selection of the specific controls very quickly. The types of threats are quite well known, it is felt, because they are the ones that have occurred so often within financial systems. Also, the types of controls that can be used are well known, because they have been widely used in internal control systems.

So this approach spends most of the time performing the exposure analysis and developing the list of threat/control pairs. Controls are recommended for preventing all but the most trivial of the consequences.

Management is then presented with this list of threat/control pairs and is asked to choose which controls should be used.

Management, in turn, may be overwhelmed by this list and may have no idea of what all of the direct and indirect costs of the control system may be. So only a relatively few of the controls may be installed, for what management feels are the most urgent needs, and the others are postponed for 'further consideration.'

This, then, is the bottom-up approach, as we see it.

Top-down approach

The top-down appoach represents a quite different viewpoint from the one just discussed. For instance, it starts with a *much* broader view of the problem area. Also, it considers many types of threats—not only the well-known threats to financial records but also many types that management may not have considered systematically in the past.

To illustrate what is meant by the top-down approach, consider the 'vulnerability analysis' seminars developed at SRI International of Menlo Park, California (Reference 6). These are one-day seminars that have been conducted for organizations of many sizes, ranging from small, single product companies to large-size corporations. The seminars involve groups of from 8 to 12 executive, in an environment where they will be able to give full attention to the subject (no interrupting phone calls, etc.).

A vulnerability analysis seminar begins by first identifying the 'underpinnings' of the company—those supportive factors upon which the successful operation of the company depends—and the possible threats to those underpinnings. Each underpinning is examined from the standpoint of the harmful consequences that could result if it were suddenly removed, changed, or obsoleted.

SRI has classified these underpinnings into twelve categories. Some of these are: (1) the resources used (employees, raw materials, energy, etc.), (2) technologies used in the company's products, (3) the markets for the products, (4) political factors (such as government regulations that apply and possible new regulations), (5) societal factors (such as the work ethic of employees), (6) economic factors (such as inflation and recessions), and so on. SRI reports that executives often tell them they have never before really looked at all of the factors upon which their businesses depend.

This study of possible threats to underpinnings is brought home very strongly indeed when the executives start to think of some rather recent industrial casualties. For instance, hand calculators have just about wiped out the market for slide rules. Digital watches are supplanting mechanical ones at a fast rate. Recent droughts had significant impact on swimming pool construction. Motor fuel rationing has an immediate and severe impact on the travel industry, hotels and motels, recreational vehicle sales, and so on. And these are only some of the casualties.

By examining the possible threats to their company's underpinnings, executives may be brought face-to-face for the first time with serious consequences that they had not considered before.

As the next step, each participant considers each threat and records his/her evaluation of (1) how likely it is to occur and (2) what the consequences might be if it did occur. Then, by discussion, the group attempts to reach a consensus on these two points. As a result of this step, priorities are developed which help management decide which threats deserve further attention.

Clearly, the above topic is much broader than the subject of this report. Threats to managers' information is just a subset of this broad consideration of threats. The top-down approach says, in effect, that management should recognize that threats exist to a company's well-being, that the current protective measures may not be adequate, and that the subject deserves the attention of all levels of management. The threats to data and information are just a part of this overall picture.

To focus the discussion on the subject of managers' information, let us consider briefly some of the implications of the new U. S. foreign corrupt practices act, as reviewed by Baruch in Reference 7. As Baruch says, the act is not limited to foreign activities nor is it limited to illegal practices. Even some innocently-intended activities can be penalized under the act.

One of the key features of the act is the penalties imposed for 'inadequate' disclosure in the company's books and records of transactions that are financially material or that bear on the integrity of management. The Securities and Exchange Commission may insist upon the accurate and fair documentation of such transactions, in a manner that calls a reviewer's attention to possible illegality or impropriety. Further, these transactions are not defined; what may be a legal business practice today may have to be flagged as 'possibly illegal' from now on.

The types of transactions that should be so flagged include within-company ownership of a supplier company, receiving rebates from customers, transferring money outside of the U.S., and the making of legal political contributions.

If such transactions are not 'accurately and fairly' documented (and those terms are not defined in the law), the books and records may be deemed to be materially deficient and the management can be prosecuted. Further, to convict, the government has only to show that the records were deficient because of some deliberate action or inaction on the part of the executive(s). The government does not have to prove an intent to violate the law.

The business environment may thus be changing in the direction where managers' 'personal' files (holding their business correspondence, memos, appointments, and so on) will take on even greater archival importance. Information in managers' files may be needed to prove innocence. In this kind of non-benign environment, managers will not want others to be able to read, insert, delete, or change information in their files.

In brief, the types of threats that have historically occurred against financial systems, and the types of controls used to protect against those threats, may not adequately cover the situation for the office of the future. It would be well, we think, for management to take a broader look at the vulnerabilities and risks.

Vulnerability/risk analysis

It probably is not possible to give *complete* protection against even one type of threat, and it is not practical to try to give some protection against every conceivable type of threat. So the design of a security system involves setting priorities, to indicate where attention is to be directed.

To help in setting these priorities, a vulnerability/risk analysis can be employed. It, in turn, divides into several parts. We will discuss the subject in terms of threats to managers' information.

Vulnerability analysis. For this study, we believe that something like SRI's vulnerability analysis seminar would be appropriate, *at the data and information level.* That is, a top-level seminar might be conducted first, along the lines discussed earlier, which looks at the threats to company underpinnings. Then the process might be repeated at lower levels of management, where such an analysis is felt to be needed. We are arguing here that one such area that needs attention is that of 'data and information.' As with the other seminar, this might involve, say, six to eight managers and might last the better part of a day.

The group would seek to develop a list of threats to information, and to the information system. These threats would include the deliberate or accidental modification, destruction, or disclosure of information. One good source for starting such a list is a report prepared by SRI International for the U. S. National Bureau of Standards, Reference 4c.

The next step would be to give a rough appraisal of the current protection against each type of threat. This will require someone in the group having some knowledge of the current state of the art in protection mechanisms. As we have pointed out in numerous previous reports, today's operating systems are fairly vulnerable. Just about every well-planned attempt to penetrate an operating system has been successful, we are told.

Then the group should try to identify some of the consequences of those threats coming to pass. The exposures can include direct losses, indirect losses, and loss of prestige if a penetration becomes publicly known.

The threats, the weaknesses in protection against those threats, and the consequences if those threats come to pass constitute the vulnerability analysis, as we see it.

Risk analysis. The next step is for the group to assess the likelihood of those threats materializing. This step will be largely subjective. As discussed earlier in this report, some statistics on detected and reported data security violations have been published. But these statistics apply to a different environment (typically, central batch data processing systems) and may not be too pertinent for the analysis being made here.

Risk is measured as a probability—the likelihood of an event occurring within some specified time period. In the final analysis, it will be a guess. "I think that there is about one chance in a hundred that someone will try to gain unauthorized access to such-and-such a file within the next year," might be an example of such an assessment.

Vulnerability/ risk analysis. This is the analysis that provides the basis for setting priorities in the security project, to indicate where controls are most needed. It brings together the following types of information.

The threats to which the organization seems to be vulnerable, at least to some extent.

The exposure for each threat—the harm or loss that the threat could bring, should it come to pass.

The risk of that threat actually occurring.

The expected loss from that threat.

The possible controls to bolster the protection against that threat.

The term 'expected loss' needs more explanation. Suppose that the likelihood of a threat actually occurring in a one-year period is estimated to be 0.1 (one tenth). If it does occur, the estimated loss would be $10,000. Within a ten year span, it is almost certain that the threat will occur and the $10,000 loss will be realized. Thus, the loss will be $10,000 in the year that the threat occurs and zero in the other nine years of the period. The expected loss is then $1,000 each year for the ten years.

The concept is valid over the long run, and provides an estimate of the average loss per year. But, of course, in any one year, one or more threats may actually materialize and the losses for that year can be substantially greater than the expected loss.

This is one reason, we suspect, why the bottom-up approach pays relatively little attention to risk analysis. The bottom-up approach, as we see it, uses a very pragmatic point of view. If an exposure is large enough, it should be guarded against, almost regardless of the likelihood of the threat occurring. Maybe the likelihood is only one chance in one hundred that the threat will occur within the next year—but it has just as great a likelihood of occurring next year as it has of occurring in, say, the fiftieth year.

Exposure *is* important, very important. But an organization simply cannot afford to protect against every eventuality. Risk must be considered also. And the concept of expected loss is also important; it says, in effect, "With the set of controls that we are using today, here is the average loss that we should expect per year for this set of threats."

In our opinion, the vulnerability/risk analysis can be very helpful in setting security requirements for managers' information.

Conclusion

It appears that one of the major areas of attention in the computer field in the next few years will be that of computer services for managers. Up to now, computers have primarily aided company operations (as well as engineering, of course); managers and executives have received only passing support.

In our report of two months ago, we discussed the variety of information handling and decision making activities that managers perform, based on some intensive studies of managerial work. Further, we indicated which of those activities might be most amenable to computer support.

Last month, we described two methods for determining what information managers need to receive, for performing their jobs. This process is the *determining requirements* step preparatory to building a managerial information system. Managerial information systems are being given the name 'executive information systems' (EIS), to differentiate them from other types of information systems.

In this report, we have tried to show that adequate security for managers' information is an essential part of these EIS requirements. Further, it is an aspect that may tend to be either overlooked or postponed. Security often gets the attention it deserves only after a significant loss has been discovered.

For those organizations that decide to determine these security requirements, we suspect that many will choose to follow what we have described above as the bottom-up approach. In essence, this approach involves either the installation of a conventional internal control system, for handling managers' information, or for bolstering an existing internal control system for that same purpose. The design and installation of an internal control system are well understood and the methods employed are well known. This approach involves relatively little participation by top management.

On the other hand, some organizations may choose to follow what we described above as the top-down approach. This requires searching out threats to the very underpinnings of the organization, as a first step, and then assessing the vulnerabilities to those threats, the possible consequences, and the likelihood of occurrance. This approach does require the active participation by top management.

Once the top-level threats have been analyzed, the approach involves moving down one or two more levels. Threats to information and data systems may be identified at the top level; more of those threats are likely to come to light when the information and data systems themselves are the subjects of the analysis.

This top-down approach probably will bring out vulnerabilities that would not be recognized by the bottom-up approach.

Given a set of requirements for an EIS, the next step is to investigate the tools and techniques that are currently available for building one. That will be our subject for next month.

REFERENCES

1. *AFIPS Security Manual*, AFIPS Press (210 Summit Avenue, Montvale, N.J. 07645). The original manual was published in 1974 and may no longer be available. A revised manual has been in preparation for some time and (hopefully) will be published this summer.
2. Chambers, A. D., "Computer abuse and its control," *EDPACS* (11250 Roger Bacon Drive, Suite 17, Reston, Virginia 22090); December 1978; p. 3-12; price $5.
3. Jacobson, R. V. "Finding hidden computer crime," *Security Management* (2000 K Street N.W., Suite 621, Washington, D.C. 20006), April 1978, p. 16-18; price $16 per year.
4. Publications of the U. S. National Bureau of Standards; order from Superintendent of Documents, U. S. Government Printing Office, Washinton, D. C. 20402:
   a. Audit and evaluation of computer security, No. 003-003-01848-1; proceedings of March 1977 invitational workshop; price $4.
   b. The proceedings of the November 1978 invitational workshop on "Audit and evaluation of computer security II: System vulnerabilities and controls" had not been published as we went to press. It should be available in the next few months. For further information, contact NBS, Mail Code 640.01, Washington, D. C. 20234.
   c. An analysis of computer security safeguards for detecting and preventing intentional computer misuse; Stock no. 003-003-01871-6; January 1978; price $2.40.
5. *Auditor's study and evaluation of internal control in EDP systems*, AICPA (1211 Avenue of the Americas, New York, N.Y. 10036), 1977; price $4.50.
6. The vulnerability analysis process was developed under the auspices of SRI International (333 Ravenswood Avenue, Menlo Park, Calif. 94025). The originator (while at SRI) and foremost practitioner is Douglas Hurd (Suite 205, 801 Welch Road, Palo Alto, Calif. 94304).
7. Baruch, H., "The foreign corrupt practices act," *Harvard Business Review* (Reprint Department, Soldiers Field, Boston, Mass. 02163), January-February 1979; p. 32 ff; price $3.

EDP ANALYZER is published monthly and copyright© 1979 by Canning Publications, Inc., 925 Anza Avenue, Vista, Calif. 92083. All rights reserved. While the contents of each report are based on the best information available to us, we cannot guarantee them. Photocopying this report for personal use is permitted provided that payment of stated per-copy fee of $2.00 is made to Copyright Clearance Center, P. O. Box 8891, Boston, Mass. 02114, using fee code 0012-7523/79/070001-13$02.00. Subscription rates and back issue prices on last page. Please report non-receipt of an issue within one month of normal receiving date. Missing issues requested after this time will be supplied at regular rate.

SUBJECTS COVERED BY EDP ANALYZER IN PRIOR YEARS

1976 (Volume 14)

Number

1. Planning for Multi-national Data Processing
2. Staff Training on the Multi-national Scene
3. Professionalism: Coming or Not?
4. Integrity and Security of Personal Data
5. APL and Decision Support Systems
6. Distributed Data Systems
7. Network Structures for Distributed Systems
8. Bringing Women into Computing Management
9. Project Management Systems
10. Distributed Systems and the End User
11. Recovery in Data Base Systems
12. Toward the Better Management of Data

1977 (Volume 15)

Number

1. The Arrival of Common Systems
2. Word Processing: Part 1
3. Word Processing: Part 2
4. Computer Message Systems
5. Computer Services for Small Sites
6. The Importance of EDP Audit and Control
7. Getting the Requirements Right
8. Managing Staff Retention and Turnover
9. Making Use of Remote Computing Services
10. The Impact of Corporate EFT
11. Using Some New Programming Techniques
12. Progress in Project Management

1978 (Volume 16)

Number

1. Installing a Data Dictionary
2. Progress in Software Engineering: Part 1
3. Progress in Software Engineering: Part 2
4. The Debate on Trans-border Data Flows
5. Planning for DBMS Conversions
6. "Personal" Computers in Business
7. Planning to Use Public Packet Networks
8. The Challenges of Distributed Systems
9. The Automated Office: Part 1
10. The Automated Office: Part 2
11. Get Ready for Major Changes
12. Data Encryption: Is It for You?

1979 (Volume 17)

Number

1. The Analysis of User Needs
2. The Production of Better Software
3. Program Design Techniques
4. How to Prepare for the Coming Changes
5. Computer Support for Managers
6. What Information Do Managers Need?
7. The Security of Managers' Information

(List of subjects prior to 1976 sent upon request)

PRICE SCHEDULE (all prices in U.S. dollars)

	U.S., Canada, Mexico (surface delivery)	Other countries (via air mail)
Subscriptions (see notes 1,2,4,5)		
1 year	$48	$60
2 years	88	112
3 years	120	156
Back issues (see notes 1,2,3)		
First copy	$6	$7
Additional copies	5	6
Binders, each (see notes 2,5,6)	$6.25	$9.75
(in California	6.63, including tax)	

NOTES

1. Reduced prices are in effect for multiple copy subscriptions and for larger quantities of a back issue. Write for details.
2. Subscription agency orders are limited to single copy subscriptions for one-, two-, and three-years only.
3. Because of the continuing demand for back issues, all previous reports are available. All back issues, at above prices, are sent air mail.
4. Optional air mail delivery is available for Canada and Mexico.
5. We strongly recommend AIR MAIL delivery to "other countries" of the world, and have included the added cost in these prices.
6. The attractive binders, for holding 12 issues of EDP ANALYZER, require no punching or special equipment.

Send your order and check to:
EDP ANALYZER
Subscription Office
925 Anza Avenue
Vista, California 92083
Phone: (714) 724-3233

Send editorial correspondence to:
EDP ANALYZER
Editorial Office
925 Anza Avenue
Vista, California 92083
Phone: (714) 724-5900

Name______________________________

Company ______________________________

Address ______________________________

City, State, ZIP Code______________________________

____