EPA DATA TALK

Vol. 3 1980 January/February No. 1

AUDIOVISUAL TRAINING

John Staley

SDC Integrated Services, Inc., on behalf of the Management Information and Data Systems Division (MIDSD) of EPA, has contracted for audiovisual training with Edutronics/McGraw-Hill and DELTAK, Inc. These contracts supply the user communities of both the NCC and WCC with audiovisual training at no tuition. Both contracts will exist throughout FY1980.

Edutronics courses are divided into modules, individual units of training. Each module is composed of an audiovisual presentation supplemented by written materials. A module can be presented as a single unit or as part of the series to which it belongs. In addition, modules can be viewed by an individual or by a group, with or without a proctor.

DELTAK training centers on the written text, with video segments and additional textual materials used to reinforce, illustrate, and review the materials. Like Edutronics courses, individual training units can be presented separately or as part of a series. Although the lessons are designed to be viewed by as few as one student at a time, group sessions led by someone knowledgeable in the course content are strongly recommended.

Both curriculums encompass data processing, management, and communications skills and can be used for training all levels of management and technical personnel.

Training materials are available from both suppliers, and course rentals are based on the use of one module per calendar month. Requested modules must be ordered the first of the month preceding the month the module is required. Requested modules are rented from the appropriate multimedia supplier and are sent to the requester.

ADP coordinators at each EPA location are the focal points for requesting audiovisual courses. Persons interested in this training should contact their local ADP coordinators.

COMPUTERIZED LEARNING

Chuck Galle

The NCC has supported the Sperry Univac Author System for Education and Training (ASET) since June 1978, when the first locally developed course went on-line. This course, Filemanager, has been completed by over 150 students whose computer experience before the course ranged from graduate degrees in computer science to no experience at all.

ASET has advantages for both the student and management:

1. Because it is inexpensive to run, it appeals to cost-conscious managers.

2. Because it is available to the student at any time the computer is up, it allows irregular scheduling.

3. Because it presents self-paced, programmed lessons (that is, certain material must be mastered before more difficult material is encountered), the student can progress at a rate consistent with personal capabilities.

ASET is also valuable to training and educational personnel. Educators particularly interested in one-to-one relation-

(Continued on Page 3)

NCC HIGHLIGHTS

Tom Rogers

√ Air conditioning problems in the computer room have contributed heavily to both degraded stability and total system downtime. Although several steps have been taken to solve these problems, the only sure answer is to relocate equipment into the new computer space as soon as it is available.

√ A preliminary planning meeting was held with Toxic's personnel to prepare for delivery of the DEC System 2020 in early January.

√ A concentrated effort has been made toward converting to SPERRY UNIVAC Series 1100 Executive Level 36. A major part of this effort is the commitment to 8-bit tape labeling scheduled to begin December 10, 1979.

√ In response to a request from the Office of Management and Budget, an analysis is being made of all direct costs for operating the NCC data center. This investigation will identify and quantify all direct monetary costs, including those previously omitted, such as Government personnel costs and certain facility costs.

√ After visiting potential backup sites, a task force has developed a Program Evaluation and Review Technique (PERT) chart and impact analysis for implementing the final phases of the Disaster Recovery Plan. In addition to security, operations, and communications personnel, the final team will include systems analysts (who will create an operating system compatible with NCC users and with the alternate site's hardware configuration) and user support personnel (who will meet with potential users and develop necessary processors).

WCC HIGHLIGHTS

Maureen Johnson

√ Job Stream Manager for MVS. The WCC is making the Job Stream Manager (JSM) at the COMNET facilities simpler, more reliable, and easier to use. To achieve this purpose, job scheduling will be virtually the same at WCC as at NCC. Three priorities will handle day-to-day processing, and a special priority will handle jobs which need special consideration. This special priority will require the permission of the user's ADP Coordinator before the job is submitted and will allow any job to be run immediately during the day for a charge of six times the normal rate. The implementation date for the new JSM will be announced by User Memo when the schedule is established. Making the JSM simpler will ease the task of taming the MVS System and, in turn, will ensure better performance.

√ Network Problem Solved. An intensive effort from COMNET and COMTEN personnel has resolved a major network problem which caused excessive line drops during September and October and which was originally thought to be caused by trunk circuit errors. Erroneously detecting circuit problems, the COMTEN processors initiated a trunk flush operation which terminated all active users. The result appeared to be line drops to the affected users. Trunk circuit stability has increased dramatically since the problem was resolved in October.

√ Data Backup. Technical direction has been given COMNET to establish a secure offsite storage vault for sensitive WCC user and system data. Users will continue to be encouraged to protect their data through its use.

The deadline for contributions to the March/April issue of EPA Data Talk is February 29, 1980.

Galle (Cont. from Page 1)

ships find that ASET accommodates their most imaginative efforts. Also, instructors with no previous computer programming experience can easily code ASET lessons. Instructors, however, should have some understanding of programmed instruction techniques (for example, those of Jerome Lysaught, B. F. Skinner, or other educational technologists).

Following are some examples of ASET training programs developed by the User Training ASET staff. The first two are accessible without an ASET student registration. The remaining courses require individual ASET registration by the student.

- @HELP*ECL. On-line, ECL command assistance can be obtained by entering this command.
- @INTRODUCTION*NCC. Entering this command gives the student a 30-minute history and description of the NCC system: configuration, component descriptions, management organization, usage figures, and other general-interest information. This presentation is ideal for managers who have visitors interested in what the NCC is and in what it does.
- Computer Basics. This introduction to data processing describes basic components, registers, symbolic access to mass storage, operation systems, Hollerith code, and a brief history of the industry. It is aimed at data entry level for new employees and cross-discipline trainees.
- Filemanager. This course introduces concepts of the SPERRY UNIVAC 1100 Mass Storage System and discusses data files, program files, F-cycles, element cycles, read and write keys, symbiont files, and use of the Sperry Univac Text Editor.
- ECL Introduction. The next step up from Filemanager, this modular course treats the most useful ECL commands. This course and Filemanager should prepare the student to use the NCC system in all respects except that of higher-level programming languages such as FORTRAN, COBOL, PL/1, etc.

The latter three courses were developed at NCC and are being used now at over 40 other major Sperry Univac sites under distribution agreements with the USE Subcommittee on Computer Assisted Instruction.

Also available are courses developed by Sperry Univac in the programming language BASIC, the SPERRY UNIVAC CTS Processor, and the programming language COBOL.

For information regarding ASET, call User Training at (919) 541-3648 (FTS 629-3648).

BIBLIOGRAPHY OF ADP LAWS AVAILABLE FROM OMB

The Office of Management and Budget has compiled an annotated bibliography of ADP laws, policies, and regulations. Most of the material referenced in the bibliography is in MIDSD's Information Management Controls Branch files. The Office can also provide information on where to locate copies of the laws, Executive orders, OMB circulars, GAO reports, and FIPS standards.

The bibliography has been distributed to the Regional ADP Branch Chiefs, but more copies are available. If you need a copy or if you need assistance locating a document or reference, call Peg Hall at (202) 755-0800.

ADP SECURITY

Marguerite L. Hall, Computer Specialist

This is the second in a series of four articles on ADP Security. The first article reviewed the peculiarities of ADP that make it inherently insecure. This article looks at goals, the scope of ADP security, and its key concepts and terminology. Because of its length only the first half appears in this issue of EPA Data Talk. The second half discusses protection of our ADP resources, control, and risk management. The third article traces the development of awareness of ADP security in the Federal sector. The fourth article covers EPA's recently developed Agencywide security program and our plans for a staged implementation.

Core Concepts: Part I

It's probably true of all new disciplines. They emerge with fuzzy concepts, amorphic scopes, and tortured terminology. ADP security is certainly no exception. Goals are confused with policy, policy with standards, standards with guidelines, guidelines with procedures, and procedures with goals. Antonyms are transformed into synonyms. Synonyms diverge never again to meet.

ADP security just isn't all that complicated. Most of the principles are things 2-year-olds know intuitively: fire burns, objects fall, locks go with keys, accidents happen, there are good people, there are bad people, and sometimes people hit back.

With a little thought, scope can be delineated, goals set, and concepts communicated. That's the intent of this article. While the scope, goal, and concepts were worked out with EPA in mind, they probably are fully compatible with other organizations and missions. Whether an agency's products are clean air and clear water (like EPA's), or military weapons, or global secrets, or welfare checks, concerns are about the same--that is, doing something about ADP's inherent insecurities.

The scope of ADP security needs to be defined first. Scope concerns boundaries: what's out and what's in. What's not ADP is out. What's ADP is in. Data processing facilities are in. Computer hardware and peripherals are in. Telecommunications networks are in. Sensitive application systems are in. Application systems critical to EPA's mission or operation are in. Documentation is in. Personnel operating and maintaining sensitive or critical application systems are in.

On a different level, scope covers those areas of ADP which are subject to problems because of ADP's complexity, its concentrated and intangible assets, and its accessibility. In other words, those areas where you're likely to find the nondata "D's" of ADP: disruption, destruction, diversion, and disclosure.

There's also a third dimension to scope. Many security programs are structured to include data center reliability and accuracy. EPA's program doesn't include them since this dimension has already been addressed, and seems to fit better, in our various computer performance management and reliability programs.

Once scope has been carved out, goals can be defined. Goals are ideas at the head of hierarchies or at the top of tree structures. Good goals last a system's life. Goals should be coded in 25 words or less. EPA's ADP security goal meets all the above criteria. It is to:

TAKE ALL REASONABLE MEASURES TO PROTECT OUR ADP RESOURCES

Now I realise that you need to understand what's meant by "take" and "all reasonable" and "measures" and "protect" and "our ADP resources" to have the goal be anything other than a jumble of jargon. That's the intent of the remainder of this article: to explore the

underlying ideas that give the goal meaning; to make it glitter, if you will. To understand, you'll need to become familiar with eight concepts:

1. ADP Resource	3. Vulnerability	5. Likelihood	7. Control
2. Threat	4. Adverse Event	6. Risk	8. Risk Management

ADP RESOURCE comes first since it's the most basic. I like to think of this concept in terms of the structure pictured in Figure 1.

At the base you see "facilities," "hardware," "software," "data," "supplies," "documentation," "people," and "procedures." The interaction of these elements, one hopes, results in the middle layer, "service." "Service" is computer time, telecommunications, data storage, user support, and application system development and operation. "Service" to be "service" needs to be available to those authorized to receive it when they request it. "Information" is at the top of the triangle. It's the ultimate ADP resource. It's what everything else is on the floor to support.

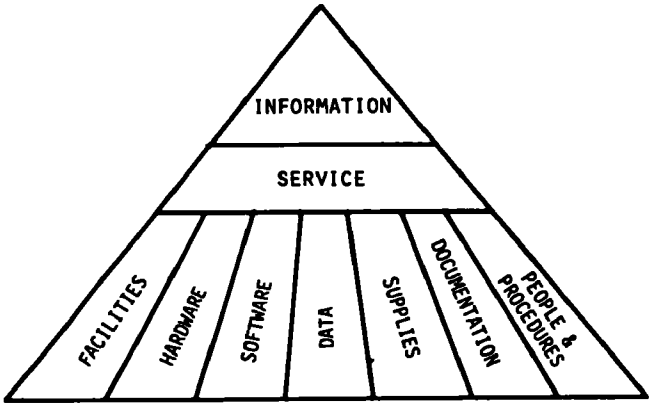

Figure 1. ADP Resource

An important thing to remember about ADP resources is that they have value which usually can be expressed in dollar terms. It costs money to reprogram and redocument. Unauthorized access costs money. Service delay costs money. An information ABEND costs money too.

The next concept is THREAT. Threats are the things that go bump in the night. Threats are out to get your ADP resources. They attack your facilities, your hardware and software, your data, supplies, documentation, people, and the procedures people follow.

In graphic form, threats look like Figure 2.

Fortunately, threats are easy to recognize. They come in just two basic forms: (1) people, and (2) change in the environment.

ADP resources have problems with people. That's because people do dumb things, unexpected things, and bad things. They steal, they subvert, they sabotage, they smuggle, they sicken, they smoke and spill Coke in computer rooms. They have maimed memory, clogged channels, torn tapes, and damaged disks. They have put bullets through the hearts of innocent CPU's.

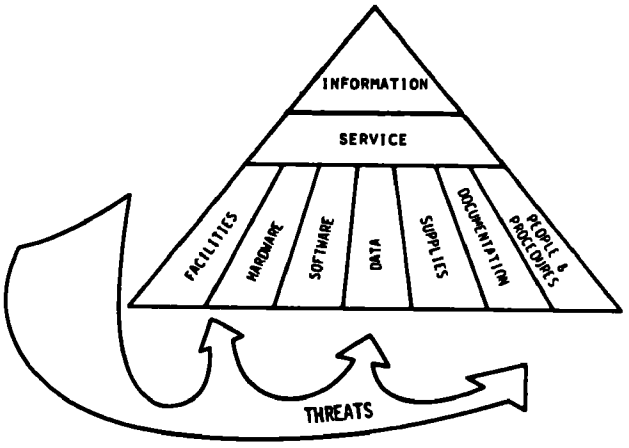

Figure 2. Threats

ADP resources are also threatened by uncontrolled change--change caused by fire, flood, heat or humidity, wind or weather, shakeup or shakedown, explosion or implosion, dust or dirt, power peak or power failure. All in all, ADP resources much prefer being kept in clean, well-lighted places.

Threats have another attribute too. They occur in finite time. "Never" is never a threat. The term used most often is "probability of occurrence." Probabilities of threats are measured in hard clock times, such as once a picosecond, once a memory cycle, once a fiscal year, or once a century. There are lots of statistics readily available on the probability of threats. NBS has maps showing the frequency of earthquakes, hurricanes, thunderstorms, and brownouts. There are publications that predict fires and floods. You can look up your chances of civil disturbances, sun spots, and accidents on Interstate 270. If you need drug addiction data, fraud facts, and sabotage statistics, they're available too.

The third concept is VULNERABILITY. Vulnerabilities look like Figure 3. Threats can't reach an ADP resource without the assistance of a vulnerability. Vulnerabilities are holes threats sneak through or the weaknesses they exploit. Vulnerabilities, unlike threats, come in many shapes and sizes. The most common form of vulnerability is poor management. It's followed closely by disorganization and disorder. Vulnerabilities can also be recognized through open-door and open-data policies, poor training, and poor morale. Inadequate or improper procedures are way up there too. If you've seen undocumented software, you've seen a vulnerability. Likewise, if you've seen unaware or unconcerned users.

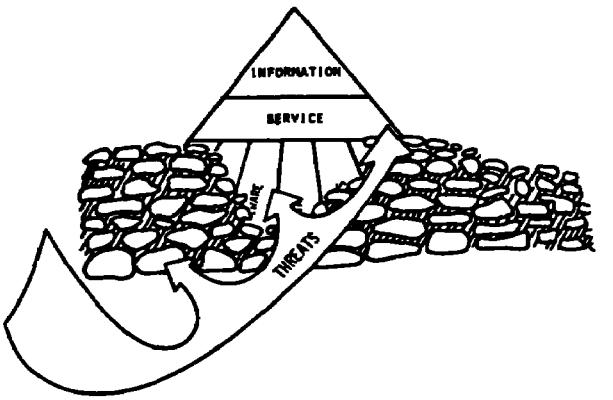

Figure 3. Vulnerabilities

ADVERSE EVENTS are the next concept. They result from the combination of threats, vulnerabilities, and ADP resources. You can't have one without the others. When a threat takes advantage of a vulnerability and does in your resource, you too can experience the thrill of an adverse event. Adverse events are roughly categorized into losses and abuses.

Losers first. You can lose facilities. you can lose hardware. You can lose software and data. You can lose supplies and documentation. You can lose key staff. The grand total is often denial of service and, ultimately, of access to the information you need when you need it.

Abuse equates to the unauthorized and unwanted. It comes in the form of unauthorized access to services, of unwanted destruction or alteration of data and software. It's diverted paychecks, tax returns, and phony invoices. There's also unauthorized disclosure or diversion of confidential information.

Figure 4 is an adverse event. You have an adverse event when rioters take over your data center. It happened recently in San Francisco. You have an adverse event with every Playgirl/Playboy calendar that rolls off your line printer. You have an adverse event with every fire that burns, flood that soaks, current that surges, earthquake that shakes, and storm that interrupts. You have an adverse event with every bowling score, recipe, or doctoral thesis stored on-line. You have an adverse event when the computer science students scramble for final grades, play

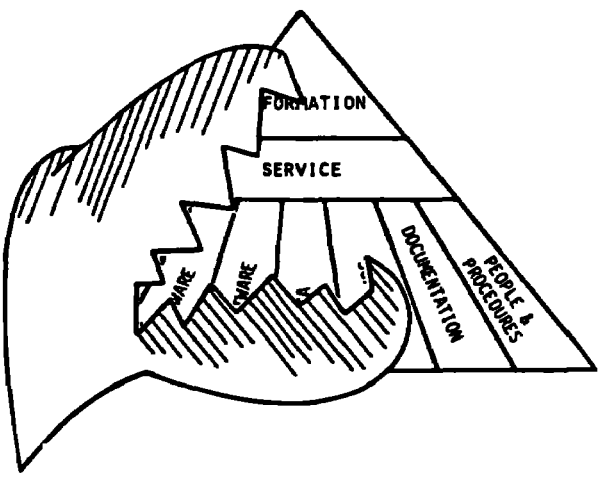

Figure 4. Adverse Event

crash-the-computer, or develop realtime, interactive, conversational, user-oriented versions of "Star Trek."

Both the next two concepts, LIKELIHOOD and RISK, relate to adverse events. Likelihood addresses chance, and risk addresses money. Like threats, adverse events also have probabilities. They're called likelihoods. If there is a probability of a threat occurring, a suitable vulnerability, and an ADP resource to be had, you have a likelihood. Where there's a river or rain or pipe or sewer or water cooler or fire department, there's the probability of an occurrence of a threat (water). For the likelihood of an adverse event (flooded equipment and supplies), you also need a vulnerability. In this case the vulnerability could be no drain or no sump pump or no rolls of plastic sheeting mounted in the computer room. The plastic, however, doesn't do much good if there are no scissors handy for cutting. One installation drowned discovering that vulnerability.

Figure 5 pictures the difference between threat probabilities and likelihood.

Likelihoods, like threats, occur in real time. The calculation of likelihood is a bit trickier than coming up with the probability of a threat, though. That's because assessing vulnerability is often pure judgment call. You can dial your local precinct and get crime statistics, but what's the likelihood of the intruder arriving at your facilities just when your guard is asleep at the closed circuit screen?

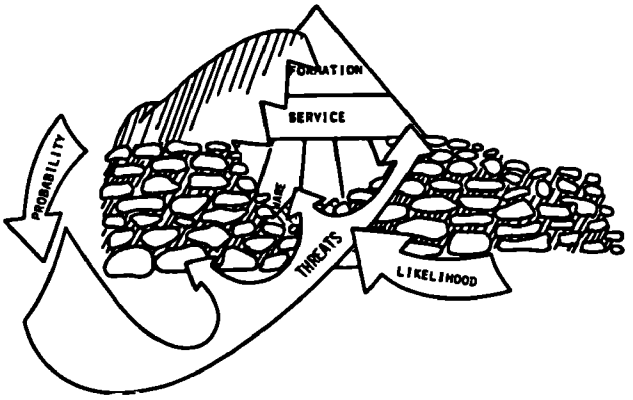

Figure 5. Difference Between Threat Probabilities and Likelihood

Risk tells you about the cost of loss or abuse from an adverse event over time. The first question is: What's the value of the ADP resource that will be abused or that you'll lose if a given adverse event occurs? The second question involves likelihood: How often can you expect that particular adverse event to occur? Remember, the adverse event results from a particular threat exploiting a particular vulnerability. It's very specific reasoning. Obviously, the greater the value of the ADP resource and the more likely the adverse event, the greater the risk.

If you're the IRS, you worry a whole lot about the integrity of your systems programmers. If you operate a data center in Washington, D.C., you don't lose a lot of sleep over earthquakes.

In Figure 6 I've taken a few liberties with the classic illustration of likelihood and worry.

Risks are usually expressed in terms of dollars per year. After all, that's how we budget. Your risk might be $1,000,000 per year from a major fire to your data center or $5,000 a year from the theft of computer time. There are various short cuts and formulas available to compute risk. NBS has put out FIPS PUB 31 that points the way. It's all very workable --that is, once you've come to terms with "likelihood."

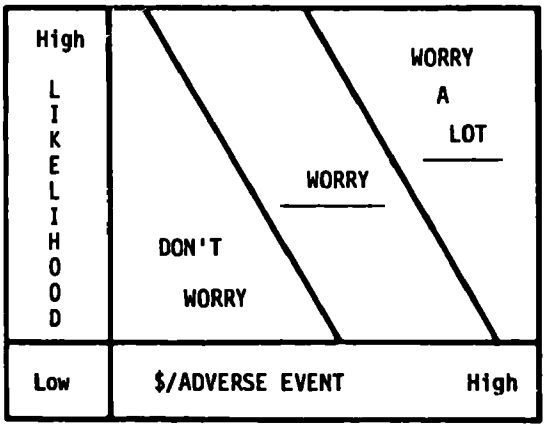

Figure 6. Likelihood and Worry

CONFERENCE

Southern Pines, NC

February 11–15, 1980

UNITED STATES
ENVIRONMENTAL PROTECTION AGENCY
National Computer Center
Research Triangle Park
North Carolina 27711