HP 3000 SECURITY/RISK MANAGEMENT

C.W. LAZAR

C.W. LAZAR
SYSTEMS INFORMATION AND TECHNOLOGY
ARCO TRANSPORTATION COMPANY
LOS ANGELES

C.W. Lazar
Systems information and technology
Arco transporation company
Los Angeles

HP 3000 Security/risk management

Purpose

The purpose of security/risk management is
to maintain operations in planned mode
to prevent as far as practicable unauthorized
access to (discovery or modification) of
program and data files
to prevent, mitigate or recover from inside or
outside dysfunctions.

Environment

Organizations that can afford an HP 3000 and the support staff generally are significant businesses.
Edp costs vary between 1.5 pct and 5 pct of total costs and business related systems may handle 30 pct to 50 pct of company revenues.
The following system illustrate the point.

Payroll	30	pct plus
materials purchasing	30	" "
accounts payable	30	" "
materials inventory	10	" "
general ledger	100	" "

Hence a 20 Dollar a year business may run 6 to 20 million through its HP 3000
my company runs approximately 70 million through and we may double that in 12 months.
Most HP 3000 installations represent a department's first or most ambitious step into electronic data processing away from manual or service center operations.
a large portion of system managers have had little or no system management responsibilities.
This presentation is aimed at them and their concerned auditors.

2 - 1

2. The fundamental security devision rule
decision about security measures should be based on cost versus worth. An organization shouldn't spend more to avoid

an increase than the libel or expected cost of the incident.
In mathematical terms
de(pic1) is greater than(de(p1'ci') plus demci)
where
de equals discounted expected value
pi " " probability of incident i
c1 " " cost of incident i
mci " " cost of mitigation measures for incident i
No absolutes
The cedision rule is not a new or original concept. It is a game theory rule that emphasizes that there are no absolutes.
That measures short of suicide can't eliminate undesired incidents: they can only reduce theire probability on their cost.
Consider a fire in the computer room. It can be caused by a dropped cigarette or an electrical short or an overheated cooling fan or arson or a fire in the next room or one probagated through the plenum or false floor. Rules can ban smoking but not electrical shorts.
2 - 3
Paperless computer rooms can reduce the source of fuel and halon systems can reduce the source of oxygen. But how often is the computer room the first source of fire in a building. How many computer rooms share buildings with chemical closets used by cleaning personnel or oily rags used by engineers?
How many computer centers are built on bed rock with fire proof walls and no common air conditioning equipment?
How well will these fire retardent measures combate and enternally sourced fire and which more probable?
2 - 4
The probability of a computer room fire is very low on the order less than 0.1 pct per year. The cost of an automatic halon system is 4000 to 10,000 for a 10' x 15' room. It would imply that the cost of the fire totally suppressed should be

4000/.001
or
4,000,000
if back-up tapes are stored off-site and there is a back-up computer access agreement, then it is unlikely that the cost of a total hardware loss fire would equal 4,000,000.
It follows that an expensive automatic halon system may be a waste of stockholders' money for a business data processing machine. This of course may not be true for a real time process control computer or an airline reservation system.
This is a reasonable example of applying the decision rule. It of course doesn't leave the auditors with a sanguine feeling, that I placated by installing a 60 handcarried halon system.
3. Quantification of security costs
Decisions about security need to be couched in reasonable estimates of costs of security systems and probabilities of undesired incidents.
3.1 Security systems costs.
Security systems can be divided into two arbitrary classes
probability reducers
cost mitigators
The following are examples of probability reducers, their objectives and ball park costs.

item	objective	cost range	comment
computer room locks	reduce unauthorized access	150- 1000	cheap looks can be jimmied, with credit card
door locks	reduce unauthorized access to files reduce probability of theft	100- 300 one time	beveled latches can be jimmied with credit card

item	objective	cost range	comment
sentries	reduce unauthorized access to files reduced probability of thef	10,000- 20,000 per shift per year	cheap sentry can become thief can become lazy
passwords account, group, user	reduce unauthorized access to files and programs	1.00- 5.00 per password per change	effectiveness is inversely proportioned to age and number of cognocenti approaching

item	objective	cost range	comment
			zero after three days. Low cost and low effectiveness
			paswords are stored in clear text in stream jobs that are not lock worded and in image schema that are not lock worded.
			Multi user paswords obviate accountability

item	objective	cost range	comment
terminal locks	keep unauthorized users from accessing system	50- 400	can be bypassed with second terminal reconnected to same port.
no smoking	reduce fire probability reduce disk wear	1 to?	some smokers will violate rule. Some may quit.
manual fire extinguisher	put out fire	50- 200	Good for limited fire. Doesn't work without operator.
tape back-up system	recover lost files	15 to 50 per tape per day plus re-entry cost at 1/2 a day per person	Typically half a week day will be lost and will have manually re-entered back-up tapes

item	objective	cost range	comment
			Should be stored remotely. Need protection system.
remote tape storage	protect back-up tapes from local dysfunction	2- 10 per month per tape	Should be tested episodically
hardware insurance	recover costs of disaster	2 to 5 pct of most large companies hardware 1.5 to 3 times costs the expected cost of the disaster	self-insured. Read policies carefully.

Internal

violation of privacy

manipulations

fraud ghost vendors and employees

theft or hardware, information

External

- fires
- earthquakes
- bombings
- power failures
- toxic spills
- phone system failures