

I N S T A L L A T I O N D E S I G N
=====
A N D
O P E R A T I O N C O N S I D E R A T I O N S
=====

Longs Drug Stores: an example

by: Bill Gates

LONGS DRUG STORES, INC.

- 114 STORES LOCATED IN CALIFORNIA, HAWAII, ALASKA AND ARIZONA
- \$550 MILLION SALES IN FISCAL '78
- 5200 EMPLOYEES
- DECENTRALIZED OPERATION - NO CENTRAL WAREHOUSES

HARDWARE CONFIGURATION

ONE HP3000 SERIES II MODEL 9 WITH:

- 512 BYTES MAIN MEMORY
- ONE HP7905 SYSTEM DISC
- ONE HP7905 SPOOLER DISC
- THREE 47M BYTE ISS DISCS
- TWO 223M BYTE TELEFILE (AMPEX) DISCS
- THREE 1600 BPI TAPE DRIVES
- ONE 1250 LPM LINE PRINTER
- TWO 200 LPM LINE PRINTERS
- ONE HP2635 SYSTEM CONSOLE
- TWO TI 743 HARD COPY TERMINALS
- ONE DIABLO HARD COPY TERMINAL
- 24 HP2640 (44) CRT TERMINALS
- TWO SELECTOR CHANNELS

TWO HP2100 DOS-TCS SYSTEMS WITH:

- ONE 4M BYTE DISC (EACH)
- 14 HP2640 CRT-TERMINALS (EACH)
- ONE 1600 BPI TAPE DRIVE

TWELVE DATAPoint 1500 DISKETTE TERMINALS

APPLICATIONS

ACCOUNTS PAYABLE - 7000 INVOICES/DAY

PAYROLL - 5200 EMPLOYEES PAID WEEKLY

ACCOUNTS RECEIVABLE - 4000 TRANSACTIONS/DAY

GENERAL LEDGER

FINANCIAL REPORTING

CASH RECEIPTS

INTER-STORE TRANSFERS

INVENTORY

PHARMACY DRUG INFORMATION

ASSETS/DEPRECIATION

WORK PROCESSING

COM (MICROFICHE)

OPERATING SCHEDULE/MIX

3 SHIFTS - 5 DAYS/WEEK

DAY SHIFT - ALL TERMINAL WORK

- TYPICAL 12 - 20 SESSIONS, ONE-TWO JOBS

NIGHT SHIFT - HEAVY BATCH 3 - 4 JOBS

GRAVE SHIFT - LIGHT - MODERATE BATCH - "CLEAN-UP"

SOFTWARE IN USE

- 95% COBOL
- 5% SPL AND BASIC
- MOST DATA STRUCTURED WITH IMAGE DATA-BASE SYSTEM
- HEAVY USE OF QUERY LANGUAGE
 - BY PROGRAMMERS FOR TEST/DEBUG
 - BY USERS FOR REPORTING AND LIMITED UPDATING

ACCOUNTING STRUCTURE

- TWO MAIN ACCOUNTS:
- PRODUCTN (PRODUCTION)
- PROGDEV (PROGRAM DEVELOPMENT)

OTHERS: SYS
SUPPORT
ACCOUNT 1
PLAYLAND

PROGDEV - PROGRAM DEVELOPMENT

GROUPS

- BY APPLICATION SYSTEM

ACP, PAY, ETC.

ACPS - CONTAINS WORKING SOURCE
AND OBJECT FILES

ACP - CONTAINS ACCOUNTS PAYABLE
TEST DATA

USERS

PROGRAMMERS (NO HOME GROUP)

SECURITY

ACCOUNT. PASSWORD

PRODUCTN (PRODUCTION)

GROUPS

- PUB - ALL OBJECT PROGRAMS
- PRODUCTN STREAM FILE
 - DATA BASE SCHEMA FILES
 - (EXECUTE ACCESS TO ANY)
 - (OTHER ACCESS TO AL, AM)

- SOURCE ALL PRODUCTION SOURCE
- (READ ACCESS TO ANY)
 - (OTHER ACCESS TO AL, AM)

XEQ ALL QUERY XEQ FILES

APPLICATION GROUPS

PAY, ACP, ETC. ALL DATA FILES
AND QUERY PROC.FILES

USERS

MGR - USED INFREQUENTLY

AL - RUNS MOST JOBS

STANDARD USERS (OUTSIDE EDP DEPT)

EXCEPTIONAL USERS (PROGRAMMERS)

NOTE: ALL PROGRAMS RUN FROM
APPLICATION GROUPS, ACCESSING
ONLY DATA WITHIN THE GROUP
(EXCEPT FOR CERTAIN DATA
BASES ALLOWING READ ACCESS
TO AC.

SECURITY

- A. PHYSICAL SECURITY
- B. DATA SECURITY
- C. DISASTER CONTINGENCY PLANNING
- D. AUDIT FUNCTION

BACKUP

- DONE BY STORE RATHER THAN SYSDUMP

REASONS:

- STORE MAY BE SELECTIVE
- STORE MAY BE RUN DURING OTHER PROCESSING
- MOST BACKUP DONE BY APPLICATION
 - USES SET OF GENERATION BACKUP TAPES
101ACP, 102ACP,.....120ACP ← VOLUME ID'S
 - ONLY FILES NECESSARY FOR RECOVERY (IN CASE OF CRASH) ARE STORED.
 - FREQUENCY DEPENDS UPON CHARACTERISTICS OF APPLICATION GROUP
- "SYSTEM" BACKUP DONE EACH EVENING AT 6:00 P.M.
 - FUTURE DATE SYSDUMP
 - STORE OF @.PUB.SYS
 - STORE OF @.PUB.PRODUCTN, @ XEQ.PRODUCTN, @SOURCE.
PRODUCTN.
 - STORE OF MISC. INTERACTIVE GROUPS

CONSOLE OPERATIONS PROGRAM

- READS JOB STREAMS TO TEMP FILE
- ALLOWS CONSOLE OPERATOR TO ENTER PROGRAM
"PARAMETER CARDS"
- STREAMS FROM TEMP FILE

SYSTEM MAINTENANCE

- "GOLD" BOOK KEPT
 - SYSTEM PROBLEM LOG
 - MAINTENANCE LOG
 - COPY OF SERVICE CONTRACT (S)
 - CURRENT CONFIGURATION

- "SYSDATA" JOB
 - RUN EACH MONDAY MORNING
 - CONTAINS:
 - 1) FREE 2 LISTING
 - 2) REPORT @.@ (+ RESET ACCT.)
 - 3) LISTF @.PROGDEV, 2
 - 4) LISTF @.PRODUCTN, 2
 - 5) MEMLOGAN. LISTING
 - 6) DUMMY SYSDUMP
 - 7) DATABASE UTILITY LISTING
 - REVIEWED AT DEPARTMENT MEETING

- COLD LOAD DONE EACH FRIDAY EVENING AFTER SYSDUMP
- RELOAD DONE AFTER P.M.
- WEEKLY COMPUTER SCHEDULE PREPARED

MISC. RECOMMENDATIONS

- USE "EXCESSIVE" BACKUP AT BEGINNING
- WORK WITH CUSTOMER ENGINEER - LEARN YOUR HARDWARE!
- LEARN SYSTEM UTILITIES
- MAKE FREQUENT CONTACTS WITH OTHER SITES
- SET UP COMMUNICATION METHOD TO USERS
(IN CASE OF SYSTEM CRASH OR DOWN TIME)
- "MANAGE" SYSTEM
- USE SECURITY FROM BEGINNING

DATA PROCESSING SECURITY

- I. PHYSICAL SECURITY
- II. DATA SECURITY

DISASTER CONTINGENCY PLANNING

- I. PROTECTION AGAINST DISASTER
- II. EDP OPERATION AFTER DISASTER

CURRENT PHYSICAL SECURITY AT LONGS

- RESTRICTED ACCESS TO COMPUTER ROOM

CURRENT DATA SECURITY AT LONGS

- I. STANDARD APPLICATION DESIGN CONTROLS
 - A. DIVISION OF RESPONSIBILITY
 - B. EXTERNAL INPUT AND OUTPUT BALANCING (BY USERS)
 - C. USER APPROVAL OF PROGRAM CHANGES
- II. ACCESS TO DATA RESTRICTED
 - A. PASSWORDS
 - B. USER CAPABILITIES
 - C. EDP DEPT. RESTRICTIONS
- III. DATA ACCESS "AUDITABLE"
 - A. EDP AUDITOR
 - B. JOBS MUST "TIE TOGETHER"
 - 1. JOB REQUEST SHEET
 - 2. \$STDLIST
 - 3. CONSOLE LOG
 - 4. SYSTEM LOG

DISASTER CONTINGENCY PLAN

- I. PROTECTION AGAINST DISASTER
 - A. HALON FIRE PREVENTION SYSTEM
 - B. OFF SITE BACK-UP OF FILES
- II. EDP OPERATION AFTER DISASTER
 - A. BACK-UP SITES FOR COMPUTER
 - B. BACK-UP LOCATION FOR USERS

HOW SECURITY WAS "INSTALLED"

PHYSICAL

- WAS WIDE OPEN, GRADUALLY CLOSED IT OFF
- PHYSICAL ALTERATIONS
- INCREASED OPERATIONS PERSONNEL
- SET UP FORMAL PROGRAM TESTING PROCEDURES

DATA

STEPS IN CHRONOLOGICAL ORDER:

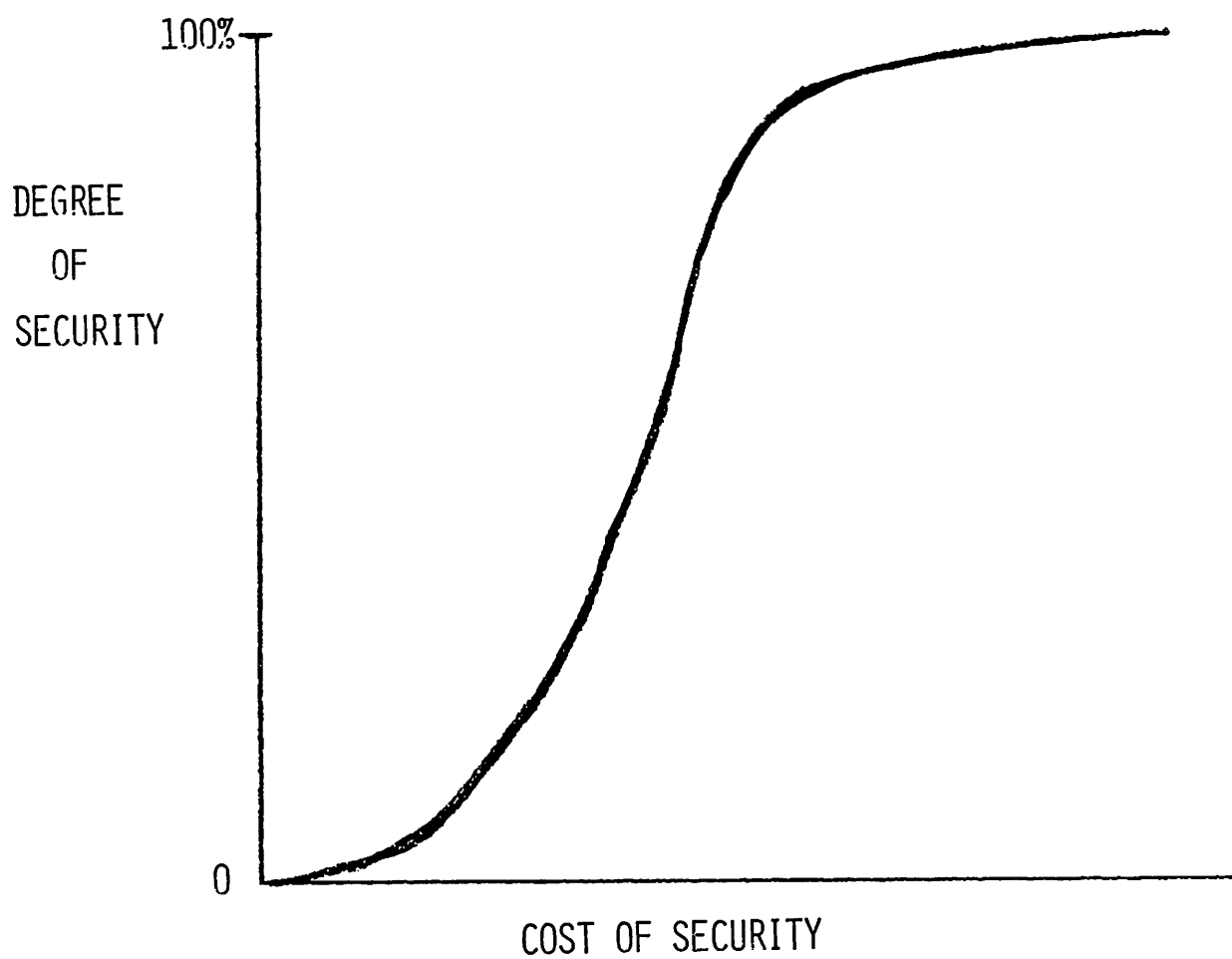
- SET UP "OPEN" PASSWORD SYSTEM
(EVERYONE KNEW PASSWORDS)
- STARTED SYSTEM LOGGING
- JOB CONTROL TIGHTENED
- SET UP MECHANISM FOR PASSWORD MAINTENANCE
(BUT KEPT PASSWORDS "OPEN")
- SET UP FORMAL PROGRAMMER "SIGN-OUT" OF PRODUCTION
DATA FOR TESTING - INCLUDED AUDIT
- CLOSED OFF PRODUCTION PASSWORDS TO PROGRAMMERS AND
USERS (EXCEPTING THEIR OWN).

- DEVELOPED CONSOLE OPERATOR PROGRAM WHICH "INSERTS CORRECT PASSWORDS INTO JOB STREAMS - CLOSED OFF PASSWORDS TO OPERATIONS (EXCEPT FOR CONSOLE OPERATOR PASSWORD)
- OBTAINED ENOUGH DISC SPACE TO GIVE PROGRAMMERS SEPARATE "TEST" DATA BASES.
IN PROGRAM DEVELOPMENT ACCOUNT - DEVELOPED UTILITIES TO HELP.

REMAINING "HOLES" IN SECURITY

- TEST FILES MAY HOLD CONFIDENTIAL DATA
- LOG RECORDS DO NOT INDICATE IF A FILE HAS BEEN MODIFIED.
- LACK OF LOG INFORMATION FOR STORE/RESTORE UTILITY

COSTS OF COMPUTER SECURITY



SUGGESTIONS FOR IMPLEMENTING SECURITY

- 1) USE GRADUAL PHASES
- 2) INVOLVE EDP AND USER PERSONNEL
 - EXPLAIN "TRADE-OFFS"
 - CHALLENGE PERSONNEL TO DEVELOP GOOD COMPROMISES BETWEEN SECURITY REQUIREMENTS AND EFFICIENT OPERATIONS.
 - EXPLAIN THAT LARGE "LOOP-HOLES" WILL EXIST DURING IMPLEMENTATION.
- 3) EXPECT VARYING DEGREES OF PERSONNEL RESISTANCE, RIDICULE, AND HOSTILITY. THIS SHOULD DECREASE OVER TIME.

PERSONNEL OBJECTIONS TO SECURITY PLAN

OBJECTION: "THIS WHOLE SECURITY SET-UP IS A SHAM BECAUSE OF (ANY LOOPHOLE)! IT IS NOT PERFECT, SO IT IS WORTHLESS."

ANSWER: MOST EDP INSTALLATIONS ARE WIDE OPEN AS FAR AS SECURITY. EXPERIENCED COMPUTER CRIMINALS ARE LOGICAL PERSONS AND WOULD PREY ON THESE SHOPS RATHER THAN ONE WITH EVEN A MODEST ATTEMPT AT SECURITY. INEXPERIENCED COMPUTER CRIMINALS CAN BE INTIMIDATED BY LESS-THAN PERFECT SECURITY PRECAUTIONS.

OBJECTION: "THESE SECURITY PROVISIONS WILL MAKE MY WORK LESS CONVENIENT AND INEFFICIENT."

ANSWER: TRUE - HOWEVER, OUR COMPANY HAS CHOSEN TO ACCEPT THE COSTS INVOLVED WITH MAKING OUR INSTALLATION SECURE. IT'S UP TO US TO MINIMIZE THOSE COSTS.