Employment Practices & Policies

CSH6 Chapter 45

"Employment Practices & Policies"

M. E. Kabay & Bridgett Robertson

Topics in CSH6 Ch 45

- What's the Problem?
- Cases
- Hiring
- Management
- Termination

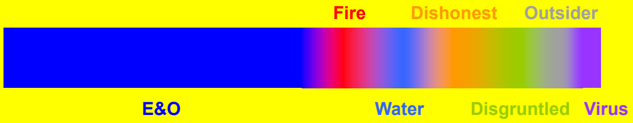
What's the Problem?

What's the Problem?

- Human beings are at the core of information assurance
- Employees who are trusted can bypass normal security controls
- Dishonest people are good at fooling others into trusting them
- Anyone with physical access to computer systems has virtually complete control

Threats Before 1993

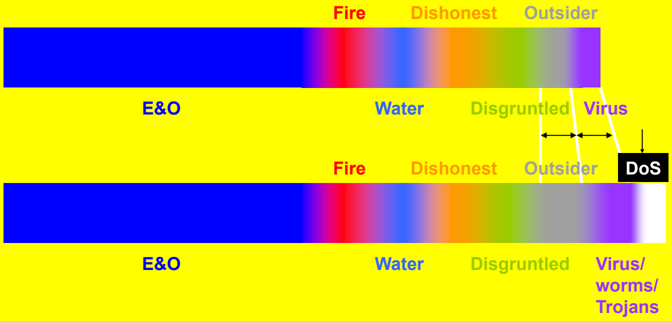
Rough Guesses About Threats to
Computer Systems & Data before the Internet Explosion



- Fuzzy borders
  - ❑bad information about computer crime
- Problems of ascertainment
  - ❑noticing violations
  - ❑reporting
  - ❑consolidating information

Threats After 1993

Rough Guesses About Threats to
Computer Systems & Data linked to the Internet



See http://www.mekabay.com/methodology/crime_stats_methods.pdf

Some Notorious (Old) Cases of Employee Malfeasance

- Diddling: New York City tax records
- Sabotage: CA Dept Info Tech
- Sabotage: Gateway2000
- Diddling: Thick Salami at Taco Bell
- Diddling: Embezzlement
- InfoWar: Industrial Espionage
- Data Loss: Stanford
- Data Diddling: SSA
- Embezzlement: 1998-12
- Logic Bomb: 2000-02
- QA: Easter Eggs in Programs
- QA: Naughty Words
- QA: UK National Insurance Registry Database Destroyed
- $2.1B for QA Failure 1999-10

Diddling: New York City tax records

Nov 96 – AP

- 3 NYC tax department employees
- Bribed by property owners from 1992 onward
- Removed records of taxes owing
- Fraudulently entered legitimate payments from innocent victims to wrong tax accounts
- Used bugs in software to cover tracks
- Stole $13M in taxes owing + $7M in interest
- Over 200 arrests

Sabotage: CA Dept Info Tech

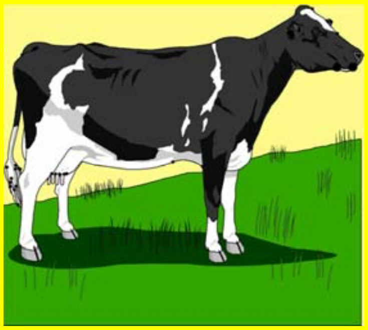
Jan 97 — San Francisco Chronicle, RISKS

- Fired subcontractor arrested
  - ❑Accused of trying to cause damage to the California Department of Information Technology
  - ❑Spent six hours online before being detected
  - ❑Crashed system
  - ❑Data restored from backups
- System management did not know the accused had been fired
- Did not alter security after his dismissal

Sabotage: Gateway2000

Jan 97 — EDUPAGE

- 20,000 copies of promotional video
- 30 seconds of pornography in mid-video
- Investigators' thinking focusing on likelihood of disgruntled employee of Gateway2000 or at video production company



Diddling: Thick Salami at Taco Bell

1997.01 — RISKS

- Willis Robinson (22 years old) reprogrammed Taco Bell cash register
  - ❑Registered each $2.99 item as costing $0.01
  - ❑Pocketed $2.98 cash per transaction
  - ❑Stole $3,600
- Management assumed error was hardware or software
- *Idiot was caught because he bragged about his theft to co-workers**
- Sentenced to 10 years in prison

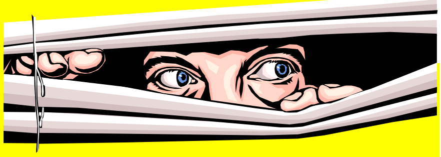
* *Criminals often caught because of THEIR errors and not because of management cleverness*

Diddling: Embezzlement

London & Manchester Assurance (1997.01)

- Jamie Griffin
  - ❑21 years old
  - ❑Clerk
  - ❑Altered records to steal £44,000
  - ❑Gambled it all away
  - ❑Claimed extortion by IRA
- Sentenced to 7 months imprisonment

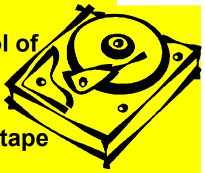
InfoWar: Industrial Espionage



Two Taiwanese arrested for espionage (June 97)

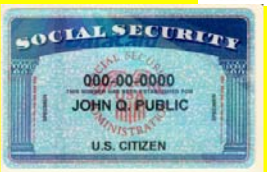
- Wanted production details for Taxol
  - ❑Ovarian cancer drug
  - ❑Worth $B
- Attempted to bribe Bristol-Myers Squibb scientist
- Employee reported to employer
- FBI arranged sting
- Both agents arrested
- Faced 35 years and 10 years in jail, respectively

Data Loss: Stanford



- Stanford University Graduate School of Business — 1998.03
- Sys admins added disks
- Reloaded files from corrupt backup tape
- Faculty & student files destroyed
- IMPLICATIONS
  - ❑*It ain't a backup if it's the only copy*
  - ❑Verify readability of backups before storing
  - ❑Make 2 backups before planned reload

Data Diddling: SSA



Social Security Administration — 1998.10

- Employee become angry with woman he had met online
  - ❑Argued in an Internet chatroom
- Used fellow-employee's terminal
- Filled in death date for woman in SSA records
- Victim applied for loan at bank
  - ❑She was "cyberdead"
- Jorge Yong admitted culpability
  - ❑Resigned
  - ❑Paid $800 in fines and damages

Embezzlement: 1998-12

China continued crackdown on computer crime

- Zhenjiang
- Two criminal hackers
  - ❑Twin bothers
- Stole 720,000 Yuan (~U$87K) from bank
  - ❑Transferred to their own accounts
- Sentenced to death (!)

Logic Bomb: 2000-02

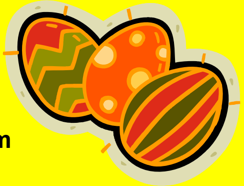
Deutsche Morgan Grenfell Inc.

- Tony Xiaotong Yu, 36, Stamford, CT
- Indicted 2000-02-10
  - ❑NY State Supreme Court, Manhattan
- Charge: Unauthorized modifications to computer system & grand larceny
- 1996: hired as a programmer
  - ❑End of 1996, became securities trader
- Accused of inserting programmatic time bomb into a risk model
  - ❑Trigger date July 2000
- Months repairing the program

QA: Easter Eggs in Programs

1998.01: Unauthorized code in commercial programs

- Major manufacturers; e.g., Microsoft
- Get through QA testing — questions about thoroughness
- Startling example: MS-Excel 97 flight simulator
  - ❑Sequence of keystrokes
  - ❑Huge color graphic images
  - ❑Real-time recalculations
  - ❑Names of development team



QA: Naughty Words

- 1998.06: Matsushita Panasonic Interactive Media
- “Secret Writer’s Society” software
  - ❑Helps kids by reading their writing
- Included extensive set of *forbidden* words (curses, etc.) intended to protect children
- Bug caused random emission of foul language from list of forbidden text
- Company denied it was a significant problem

$!*/|**!%!

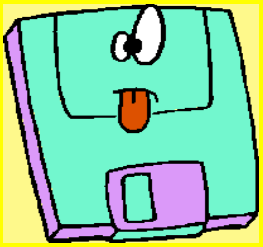
QA: UK National Insurance Registry Database Destroyed

1998.10: U.K. Department of Social Security

- Andersen Consulting installed new software
- Destroyed National Insurance Registry
- Payments had to be made by hand
- Normal checks on eligibility foregone
- Outage lasted a month
- Untold hardship for government staff and victims of delays
- Unknown losses due to fraud

$2.1B for QA Failure 1999-10

- Bug in some Toshiba laptop computers
  - ❑Allowed data corruption on diskettes
  - ❑When writing to last byte on any sector
- Toshiba settled class-action lawsuit
  - ❑Paid *$2.1B* in damages to plaintiffs*
- Serious pressure to improve QA before release in future



*Consider putting THAT on your CV! “I caused my employer $2.1 B in losses….”

NY City Police Inspector Hacks DB (2006-05)

RISKS 24.28:

- Deputy inspector altered CompStat data
  - ❑Inflated old crime statistics
  - ❑Deflated current statistics
- Intended to make himself look better than predecessor in job

Wrong Number Costs Gateway $3.6M (2002-07)

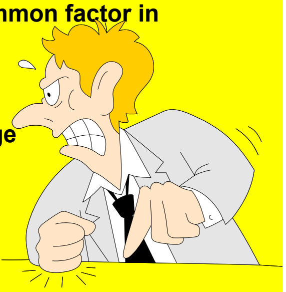
- In 1999, Gateway employee mistakenly used 800-nnn-nnnn instead of 888-nnn-nnnn for Gateway’s complaint line
- Distributed to all stores; listed on Web site; added to bills; sent to 100,000 customers
- Number was actually used by Mo’ Money distributor
  - ❑Warned Gateway within 6 days of flood of calls
  - ❑Gateway took 2 years to fix problem
- Mo’ Money awarded $3.6M in compensatory and punitive damages

Ericsson Employees Charged (2003-05)

- 3 Swedish employees of Ericsson wireless-equipment manufacturer arrested
- Charged with industrial espionage
- Accused of selling trade secrets to Russian intelligence agent
- Involved commercial, not military, products

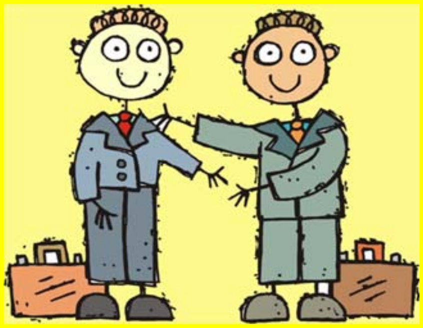
Revenge Motivates Sabotage (2005-05)

- DHS –funded study reports common factor in sabotage: revenge
- Study conducted by US Secret Service & CERT-CC
  - ❑Dozens of computer-sabotage cases from 1996-2002
  - ❑Data destruction, posting porn on Websites, denial of service. . .
- Most attackers disgruntled, angry employees or former employees
  - ❑Resented disciplinary actions, missed promotions or layoffs



Hiring, Management and Firing

- Hiring
- Management
- Termination of Employment



Hiring

- Check background carefully
  - ❑ Legal limitations on how far one can go
  - ❑ Beware *negligent hiring*
- Have candidates interviewed by future colleagues
  - ❑ Best placed to identify fakes and liars
- Enforce employment agreements
  - ❑ Legally-binding contractual terms
  - ❑ Require conformance with policies
  - ❑ Grounds for termination of employment
  - ❑ Protect intellectual property with NDA

Management

- Identify Opportunities for Abuse
- Access Is Not A Privilege or a Right
- Beware the Indispensable Employee
- Enforce Vacations
- Respond to Changes in Behavior
- Enforce Separation of Duties
- Ban Unauthorized Security Probes

Identify Opportunities for Abuse

- Think like a criminal
  - ❑Look for ways to get around controls
- Work through scenarios for possible crimes
  - ❑Develop countermeasures
  - ❑Institute monitoring procedures / audits
  - ❑Beware sole control of critical resources (see later)
  - ❑Teach employees how to respond to attempted collusion

Access Is Not A Privilege or a Right

- Do NOT allow access to become a badge of high rank
- Managers do NOT need uncontrolled access to physical computer equipment
- No one needs master keys without a reason
- No one needs access to other people's passwords or tokens
- Access can be assigned temporarily
  - ❑Specific reason (documented)
  - ❑Limited time
  - ❑With log records

Beware the Indispensable Employee

- Kabay's Law:
  NO ONE SHALL BE THE SOLE REPOSITORY OF CRITICAL INFORMATION OR SKILLS
- Having to depend on a single person for critical functions is prescription for disaster
- Extremely difficult to terminate employment of such a person
  - ❑If you tell them they are fired, they have enormous power to do harm
  - ❑If you don't have their knowledge transferred before they leave, can cause chaos

Enforce Vacations

- Vacations not only help employees, they offer an opportunity for *operational testing*
- Operations must continue in the absence of any one person
- Case:
  - ❑One client went on holiday on south-sea island without communications facilities
  - ❑Operations ground to a halt for a week

Respond to Changes in Behavior

- Any unusual change in mood / behavior warrants management attention
  - ❑Happy → sad
  - ❑Grumpy → friendly
  - ❑Relaxed → nervous
- Cases:
  - ❑Employee appears with new expensive car
  - ❑Nasty sysadmin suddenly all smiles

Enforce Separation of Duties

- No one should be able to *authorize* and also *carry out* a critical function
- Examples
  - ❑Accounting: make out check vs sign check
  - ❑Operations: add a new batch job vs launch it
  - ❑Programming: make a change vs put it into production
  - ❑Security: add a new user vs authorize addition
- Separation of duties forces *collusion* – more difficult for the criminal

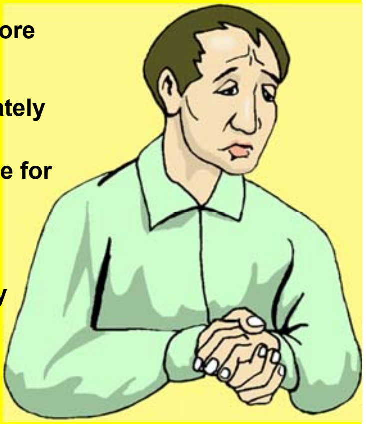
Ban Unauthorized Security Probes

- Explicitly forbid scans / probes of security posture
- No one to install unauthorized security (or other) software
- Require *written authorization** from *appropriate authority* before attempting security evaluations
- Warn all employees not to cooperate with "new security procedures" or "security checks" without verification of authority

* Known as the *get-out-of-jail card*

Termination of Employment (1)

- Resignations vs. firings
  - ❑Which do you think is more challenging for security staff?
- Shut down access immediately
  - ❑During exit interview
  - ❑Have procedures in place for complete removal of privileges for departing employee throughout entire organization
- Retrieve corporate property
  - ❑Equipment, tokens, badges, documents, forms, policies….



Termination of Employment (2)

- Principle of consistency
  - ❑Critically important to treat all employees the same way
  - ❑Cannot give a farewell party to some and frog-march others to the door
    - ✓Why not?

Review Questions (1)

1. Why should the security group work with the HR department to establish procedures for safeguarding information and information systems?
2. How can dishonest employees compromise information security? (many ways)
3. What are the key safeguards during the hiring process that can reduce risk of information security breaches?
4. Be ready to explain all of the key principles of effective employee management that improve information security as discussed in the chapter and the slides.
5. Discuss the relative difficulties of resignations and firings for security enforcement.

Review Questions (2)

6. Do some research in the *Kreitzberg Library Databases* to identify a recent case in which one or more employees caused a serious breach of security.
   - ❑ Write a 250±50 word essay analyzing the case and showing how the topics in today's lecture bear upon the case. Suggest improvements in procedures if possible.
   - ❑ POST YOUR ANSWER ON THE NUoodle MESSAGE BOARD FOR IS342 for other students to read and comment upon AND FOR EXTRA POINTS ON YOUR QUIZ GRADE.

Review Questions (3)

7. Write a portion of an employment policy that details explicitly how employees are to be treated when they are fired.
   - ❑This policy will likely have several parts.
   - ❑Expect to take about least 300±50 words for this assignment.
   - ❑POST YOUR ANSWER ON THE NUoodle MESSAGE BOARD for other students to read and comment upon and FOR EXTRA POINTS.

Now go and study