CS 523: Social, Economic, and Legal Aspects of Security

Personnel Security: Minimizing the “people risk”
What is it about?

• Everything involving employees
  – Hiring them
  – Training them
  – Monitoring their behavior
  – Handling their departure

• Why employees?
  – People who have (or recently had) privileged access cause most costly security incidents
How People Cause Problems

• Unwittingly
  – Failure to follow proper procedures
  – Forgetting security considerations
  – Lack of understanding of what they are doing

• Knowingly
  – Know what valuable info is stored, and where
  – Know the controls used, and how to defeat them
  – Motivated by greed, revenge, disgruntlement, ...
Hiring: Background checks

• Check every claim made in application form
  – Verify claims of educational achievements
    • Many cases of fake degrees from top universities who have no record of the person ever having attended, or of real degrees from bogus universities
  – Check dates of employment, investigate gaps
    • Multi-year gap as “independent consultant” often turns out to have been spent in federal prison

• Check reasons for leaving previous employers
Background checks (cont’d)

• More intensive checks if privileged access
  – Use special investigative agency
  – Criminal record
  – Credit record
• Do this for all people with privileged access
  – Including: Cleaning crews, maintenance personnel
• Inform the applicants of these checks
• Periodically re-check
Initial Training

• Procedures
  – Password selection and use
  – Physical access to computers and networks
    • Who is authorized to connect equipment, and how
  – Backup procedures
  – What can and cannot be divulged over the phone

• Appropriate and inappropriate use
  – Of computers, and of networks
  – Personal use of equipment (during & after work hours)
  – Use and ownership of email
Initial Training (cont’d)

• Import and Export of Data and Software
• Penalties for violations
• Provide copies of all course materials
  – Users should sign a form acknowledging receipt of the info (can be used later in case of litigation)
• Executives are not excluded from these classes
  – They’re just as likely to mess up (perhaps more)
  – It would send a bad message to others if they skip
Ongoing Training

• Periodically provide retraining
  – Refresher information – updates, reminders
  – A forum for employees to ask questions, express concerns, make suggestions

• Provide employees with opportunities
  – To attend workshops
  – Access to professional and trade periodicals
  – Access to reference books and other materials
Monitoring

• Especially for security-critical positions

• Identify problems, e.g., look for
  – Inappropriate use of computing resources
  – Signs of excessive stress, personal problems
  – Feeling overworked, underappreciated, ignored
  – Increase likelihood of mistakes, or departures

• Deal with problems
  – Constructively: Provide help, counseling
Monitoring (cont’d)

• Auditing of access to both equipment and data
  – Both electronic and physical (“need to know” policy)
  – Inform employees that auditing is done

• Excessive monitoring can backfire
  – E.g., duration of breaks, phone calls, web sites, …
  – Involve employees in formulating monitoring policies

• Use separation of duties
  – Employees checking for violations should be in no position to commit violations
Accountability: Who did what

- **Software related**
  - Fine-grain attribution, resists tampering (saboteur will want to cover tracks, incriminate others)
  - For development, testing, maintenance
  - Positive rewards work better (awards, etc)

- **Data related**
  - Audit trail that resists tampering
  - Forensic marking of e-data (robust vs fragile)
Handling Departures

• Departure: resigning, being fired, dying, ...
• Need for clearly defined actions to handle it
  – Shutting down accounts (exceptions in some organizations, e.g., universities for their alumni)
  – Setting up email forwarding
  – Changing critical passwords
  – Changing door access codes
  – Checking voice mail accounts
[Sometimes it’s done before employee even knows]
The “Insider Threat”

• Second most common type of security breach
  – A close second to malware
  – Far ahead of breaches by outsiders

• Prevention relies mainly on deterrence
  – Fear of detection and punishment

• Deterrence is less effective than believed
  – Perpetrators tend to have low self-control
  – Mental focus on potential benefits to themselves
Mitigation of “Insider Threat”

• Better screening of employees
  – Look for self-control, integrity

• What if an existing employee scores low?
  – Could still be highly productive and valuable
  – Move to a less sensitive position

• Decrease the temptation for all employees
  – Least privilege
  – Need-to-know
Mitigation of “Insider Threat” (cont’d)

• Organizational adoption of high standards of ethics and corporate citizenship
  – Sets the example
  – Strengthens employees’ ethical beliefs/behaviors

• Organizations with a strong culture of integrity tend to attract ethical employees
  – Employees often willing to work for lower pay (or as unpaid volunteers) in ethical organizations