CS 526: Information Security

Policy
Roles of Policy

• Internal Role: To tell employees ...
  – what is expected of them
  – how their actions will be judged

• External Role: To tell the world ...
  – how the enterprise is run
  – that there are policies supporting sound business practices
  – that the organization considers the protection of assets to be of vital importance
Employee Misbehavior: A Major Problem

• Widespread
  – Half admit to unethical behavior over previous year

• Statistically monitored and documented
  – 3 times more employee sabotage than by outside hackers

• Hurts productivity
  – In a typical large corporation, thousands of employee workday-equivalents are wasted on just one entertainment web site

• Creates liability to other employees & outside parties
  – Destroys value, bad for shareholders
Information Confidentiality

• Policy must spell out employee duties of nondisclosure and confidentiality
  – Both during and after employment
• Prohibit leakage to outsiders
  – Trade secrets
  – Price lists
  – Client lists
  – Anything towards “insider trading”
  – ...
Information Confidentiality (cont’d)

• Give examples of unintended leakage, e.g.,
  – Printing in unsecured area
  – Improper disposal of printed material
  – Logged in and unattended
  – Portable devices, removable media
  – Use of Internet
  – Use of encryption
  – Introduction of unauthorized software into company systems
Access

• **Electronic**
  – Place constraints on remote access

• **Physical**
  – Including spelling out visitor requirements

• **Minimize unnecessary access**
  – Least privilege, compartmentalization
  – “Need to know” (no snooping)

• **Software tools for enforcement**
Passwords

• Force good choice
• Force change
• Prohibit sharing
  – with co-workers
  – with outsiders (non-employees)
• Use of software tools for policy enforcement
• Include cautionary comments
  – “We will never ask you for your password”
Prohibit Hacking

• Any hacking-related activities
  – Port scans, “doorknob rattling”
  – Spoofing

• Any hacking-related tools
  – Attack tools, malware, ...
  – Prohibit both the use of known tools and the development of new tools (whether on company time/equipment or personal time/equipment)
  – Prohibit “in vitro” experimentation
• Promote appropriate and efficient use of resources
  – Prohibit others
• State clearly the allowed uses
• List examples of disallowed uses (including wasteful uses) for all resources, e.g.,
  – Computing: “no mining of bitcoins”
  – Bandwidth: “no downloading of huge movie files”
  – Printers: “no printing of sci-fi novel you’re writing”
  – Removing property from the premises
Corporate Communications

• Internal communications
  – What is and is not allowed in communications between employees (information-flow controls)

• External communications
  – How to handle communications with other businesses (partners, clients, suppliers, ... )
  – How to handle requests for information from the media (statements, interviews, ... )
  – Submission of papers, giving colloquia, ...
Employee privacy

• Employees privacy rights
  – Constitutional
  – Common-law
  – Specific laws for cyberspace

• Employee expectations of privacy
  – Might far exceed the legally specified protections
  – Valid unless policy says otherwise, and employer avoids indirectly implying otherwise (through work atmosphere, lack of enforcement, ... )
Employee privacy (cont’d)

• Can employer monitor employees?
  – Policy must address it explicitly
  – Better for document to say “may monitor” than “will monitor”
  – Employee must give consent

• Rights to privacy that are waived by employee may be deemed to hold nevertheless
  – It can happen in litigation
Employee Harassment

• Specify expected standards of conduct
  – Give specific examples of inappropriate conduct

• Prohibit “hostile work environment”
  – Include prohibition of inappropriate e-mail content and its circulation/dissemination

• Disclaim that company can completely protect employee from offensive content (e.g., viewed online)
Employee Duties of Loyalty and Care

• Duty of loyalty
  – Position should not be used for personal gain
  – Interest of organization prevails
  – “Ratting” as a duty

• Duty of care
  – Act in good faith
  – Act as a prudent person would

• Both duties are required by law from directors and officers of a corporation
Conflicts of Interest (CoI)

• Anything that *can be perceived* as corrupting an employee’s motivation or decision-making
  – A situation (e.g., personal financial/career benefit)
  – A relationship (family, dating, friendship, ...etc)

• CoIs can do damage (financial, reputational)

• Require not only disclosure, but also recusal

• Require annual signature of a responsibility statement by employee
Disciplinary Aspect

• Spell out what happens when things go wrong
  – Who is responsible for what
  – What additional procedures and investigations the responsible individuals will have to undergo
  – Who carries out the investigations
  – Sanctions (and who is responsible for applying them)
Employee Termination

• Spell out clearly defined procedures
  – Special procedures for key personnel

• Require discontinued access
  – Physical (change door keys, door access codes)
  – Electronic (change passwords)
  – Directly or via others

• Prevent taking away of resources
  – Equipment
  – Data (technical, customer lists, price lists, ... )
Other

• Backup, configuration, updates
• New software, hardware
• Data destruction (purge old, outdated)
  – Now only what & when, also how
• What to do in emergencies
  – For each type of emergency
• Business continuity plans
  – Disaster recovery, resuming operations
Compliance with policy

• Employee education program
  – Read/sign policy essential but not sufficient
• Monitoring procedures
• Enforcement procedures
• Swift action against violations
Employee buy-in

• Explain why
  – Give examples and case studies
• Employee participation / feedback
  – Via advisory committee
• “Our policy”
• Constant reminders
  – Positive (e.g., awards)
Monitoring and enforcement

- Enforcement “attitude”
- Technical enforcement tools
  - Firewalls
  - Password checkers
  - Change-detection tools
  - Intrusion-detection systems
  - ...
In case of litigation ...

- Organizations suffer harsher sentencing if they
  - have no policy
  - have policy but without proper enforcement
  - have policy with selective or discriminatory enforcement