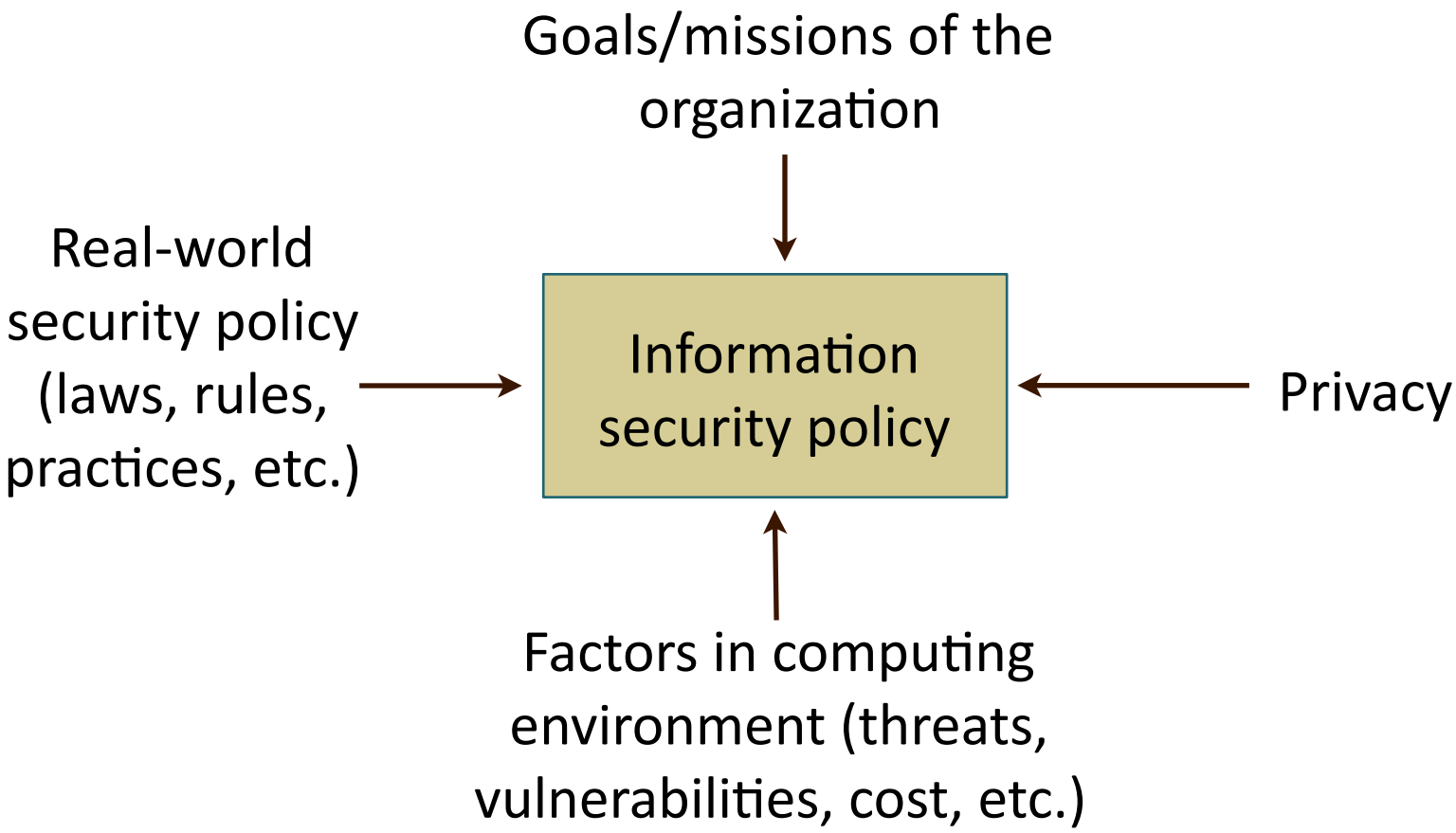
Week 2
Sources of Security Policies

Sources of Security Policy



Legal Driving Forces

Compliance Laws and Regulations
- Compliance laws and regulations create requirements for corporate security
  - Documentation requirements are strong
  - Identity management requirements tend to be strong
- Compliance can be expensive
- There are many compliance laws and regulations, and the number is increasing rapidly

Sarbanes–Oxley Act of 2002
- Massive corporate financial frauds in 2002
- Act requires firm to report material deficiencies in financial reporting processes
- Material deficiency is a significant deficiency, or combination of significant deficiencies, that results in more than a remote likelihood that a material misstatement of the annual or interim financial statements will not be prevented or detected
- Material is a mere 5% deviation
- If report material deficiencies, stock loses value, chief financial officer may lose job

Privacy Protection Laws
- The European Union (EU) Data Protection Directive of 2002
- Many other nations have strong commercial data privacy laws
- The U.S. Gramm–Leach–Bliley Act (GLBA)
- The U.S. Health Information Portability and Accountability Act (HIPAA) for private data in health care organizations

Data Breach Notification Laws
- California's SB 1386

Federal Trade Commission
- Can punish companies that fail to protect private information
- Fines and required external auditing for several years

Industry Accreditation
- For hospitals, etc.
- Often have accredited security requirements

PCI-DSS
- Payment Card Industry–Data Security Standards
- Applies to all firms that accept credit cards
- Has 12 general requirements, each with specific subrequirements

FISMA
- Federal Information Security Management Act of 2002
- Processes for all information systems used or operated by U.S. government federal agencies
- Also by any contractor or other organization on behalf of a U.S. government agency
- Certification, followed by accreditation
- Continuous monitoring
- Criticized for focusing on documentation instead of protection

Figure 2-10. Legal Driving Forces

Resources for Policy Development

- ISO 27002 (formerly 17799)
  - Code of practice for information security management
  - A comprehensive set of best practices in information security
- COBIT framework
  - Control objectives for information and related technology
  - Created by the Information Systems Audit and Control Association (ISACA)
- The Standard of Good Practice for Information Security
  - Created by Information Security Forum (ISF)

Typical Security Policy Topics

- Security involves a broad range of issues, but typically a comprehensive policy document should cover:
  - Goals/missions
  - Physical security
  - Hiring, management, and termination
  - Data protection
  - Communication security
  - Hardware, software, and operating systems
  - Technical support and maintenance
  - Privacy
  - Violation reporting

Who Should Be Involved?

- A variety of individuals should be involved in policy development
  - RFC 2196 suggests
    - Security administrators
    - IT technical staff
    - Supervisors of user groups
    - Security incident response team
    - Representatives of users groups
    - Legal counsel
    - Etc.

SYRACUSE UNIVERSITY
SUOS
CULTORES
SCIENTIA
CORONAT