Regulations

- The process of adhering to regulations is called *regulatory compliance*
- **Industry regulations** are typically developed by established professional organizations or government agencies using the expertise of seasoned security professionals
- Sample of cybersecurity regulations categories:
  - *Broadly applicable regulations*
  - *Industry-specific regulations*
  - *U.S. state regulations*
  - *International regulations*

Legislation

- Specific legislation can also be enacted by governing bodies
  - These include national, territorial, and state laws
- Due to a lack of comprehensive federal regulations for data breach notification, many states have amended their breach notification laws from the basic definitions
  - No two state laws are the same

Standards

- A standard is a document approved through consensus by a recognized standardization body
  - It provides for framework, rules, guidance, or characteristics for products or related processes and production methods
- One cybersecurity standard is the Payment Card Industry Data Security Standard (PCI DSS)

Benchmarks/Secure Configuration Guides

- **Benchmark/secure configuration guides** are usually distributed by hardware manufacturers and software developers
  - They serve as guidelines for configuring a device or software so that it is resilient to attacks
- Usually, they are usually **platform/vendor-specific guides** that only apply to specific products
- Guides are available for:
  - Network infrastructure devices
  - OSs
  - Web servers
  - Application servers

Information Sources

- There are a variety of information sources including:
  - Vendor websites
  - Conferences
  - Academic journals
  - Local industry groups
  - Social media
- A specialized research source is a **Request for comments** (**RFC**)
  - Which are white papers documents that are authored by technology bodies employing specialists, engineers, and scientists who are experts in their field