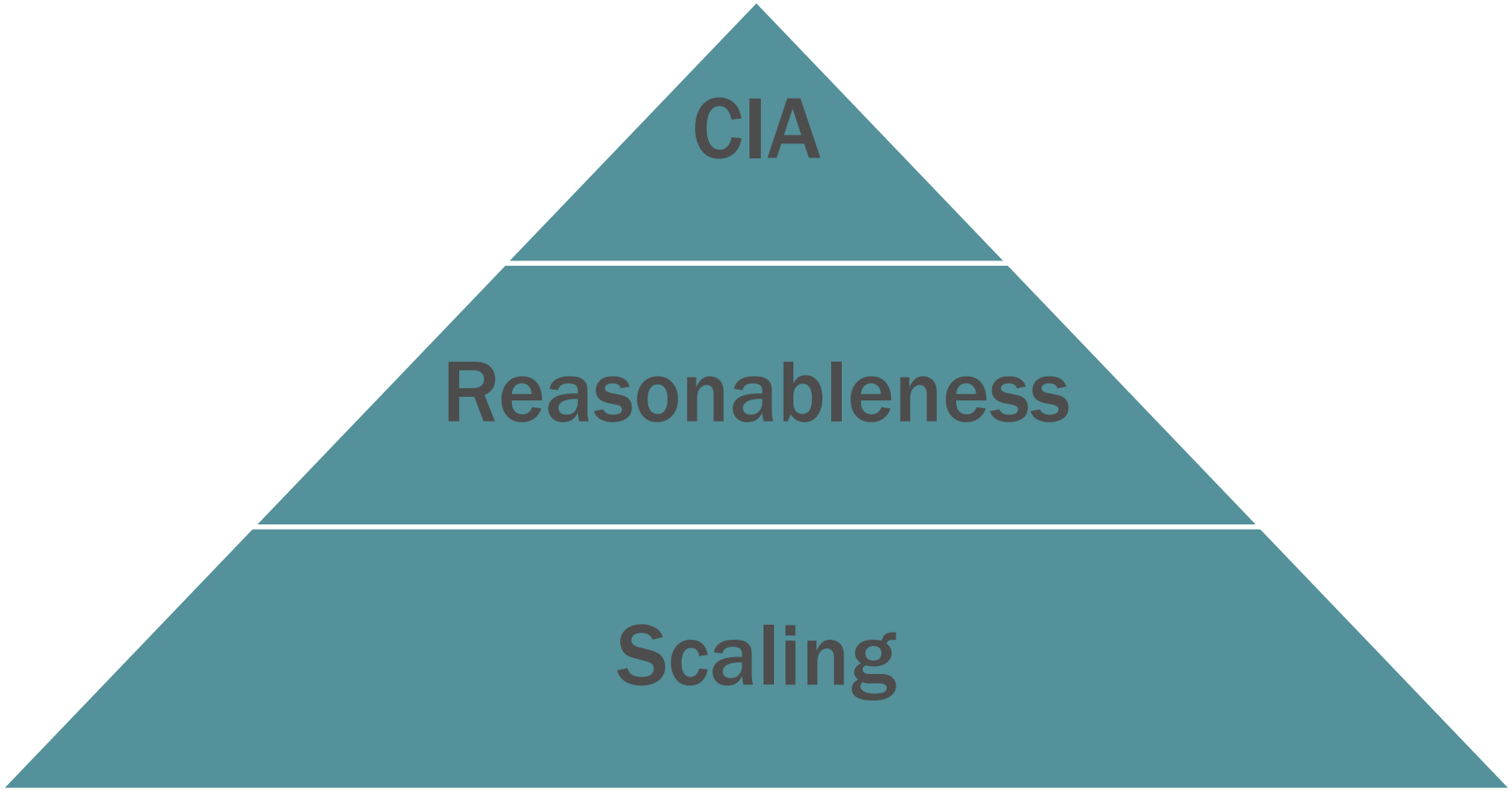
Seeing the Forest for the Trees

FOLEY
FOLEY & LARDNER LLP

Three Common Threads

- Three threads provide a broad picture of compliance obligations
  - Common standards promulgated by laws and regulations
  - Common contractual standards (PCI DSS)
  - Common industry standards (CERT at Carnegie Mellon, and the International Standards Organization)

Three Common Threads



First Common Thread

- CIA: Confidentiality, Integrity, and Availability
- CIA is a basic principle of information security
  - Data must be held in confidence
  - Data must be protected against unauthorized modification
  - Data must be available for use when needed

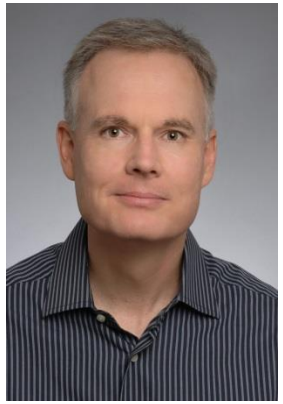
Second Common Thread

- Acting “reasonably” or taking “appropriate” or “necessary” measures to protect data
- Businesses must do what is reasonable or necessary; perfection is not required
- EU, Australia, Canada, US, and many other countries

Third Common Thread

- Scaling security measures scale with the nature of data and the risk presented
- Closely related to acting reasonably or doing what is necessary
- Security measures should reflect the sensitivity of the data and severity of the risk
- The greater the risk and sensitivity of data, the greater the effort to secure the data

Questions & Contact Information



Michael R. Overly

Partner, CISA, CISSP, COP, CIPP, ISSMP, CRISC

Foley & Lardner LLP

555 South Flower Street,

Suite 3500

Los Angeles, CA 90071

(213) 972-4500

moverly@foley.com

FOLEY

FOLEY & LARDNER LLP