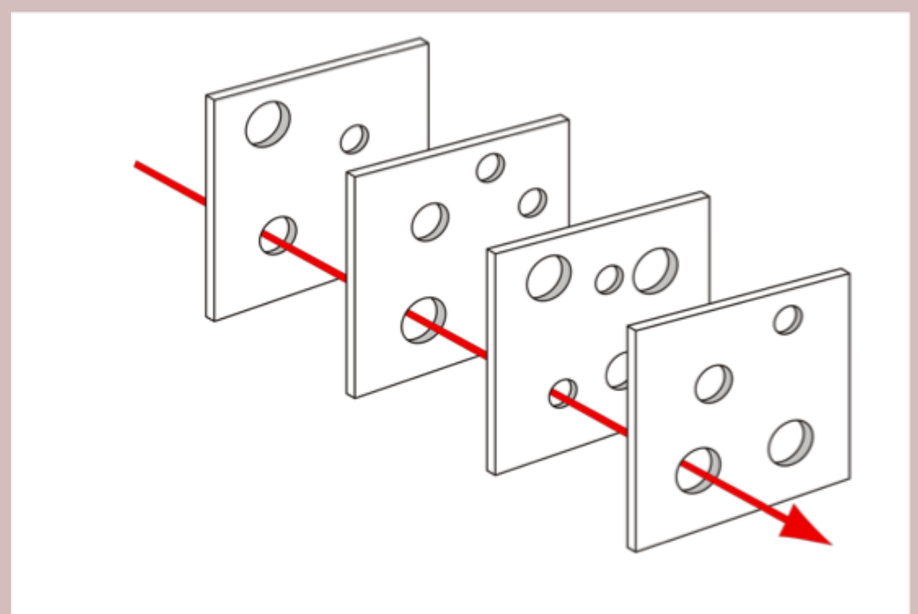
JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Defense in Depth

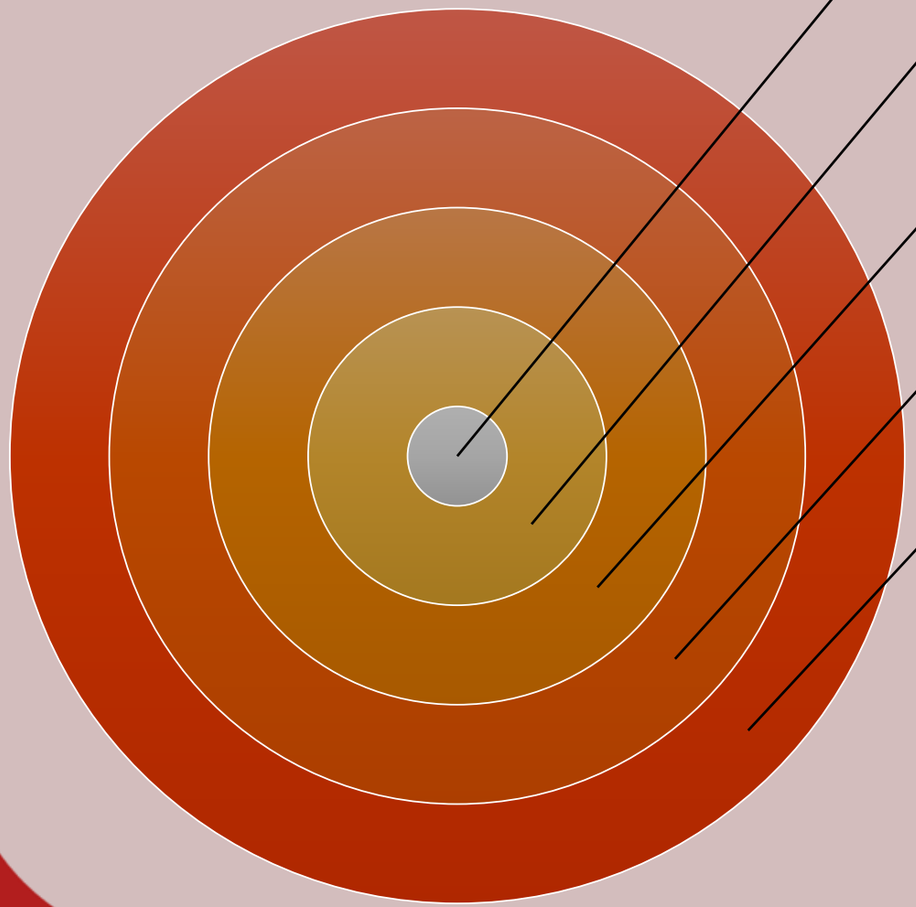
Security Architecture & Tool Sets

Defense in Depth

- Foundation of good security architecture
- Does not rely on a single defensive measure or control for protection



Layered Security Defense



Data

Application

Endpoint Security

Network

Perimeter

JASON DION

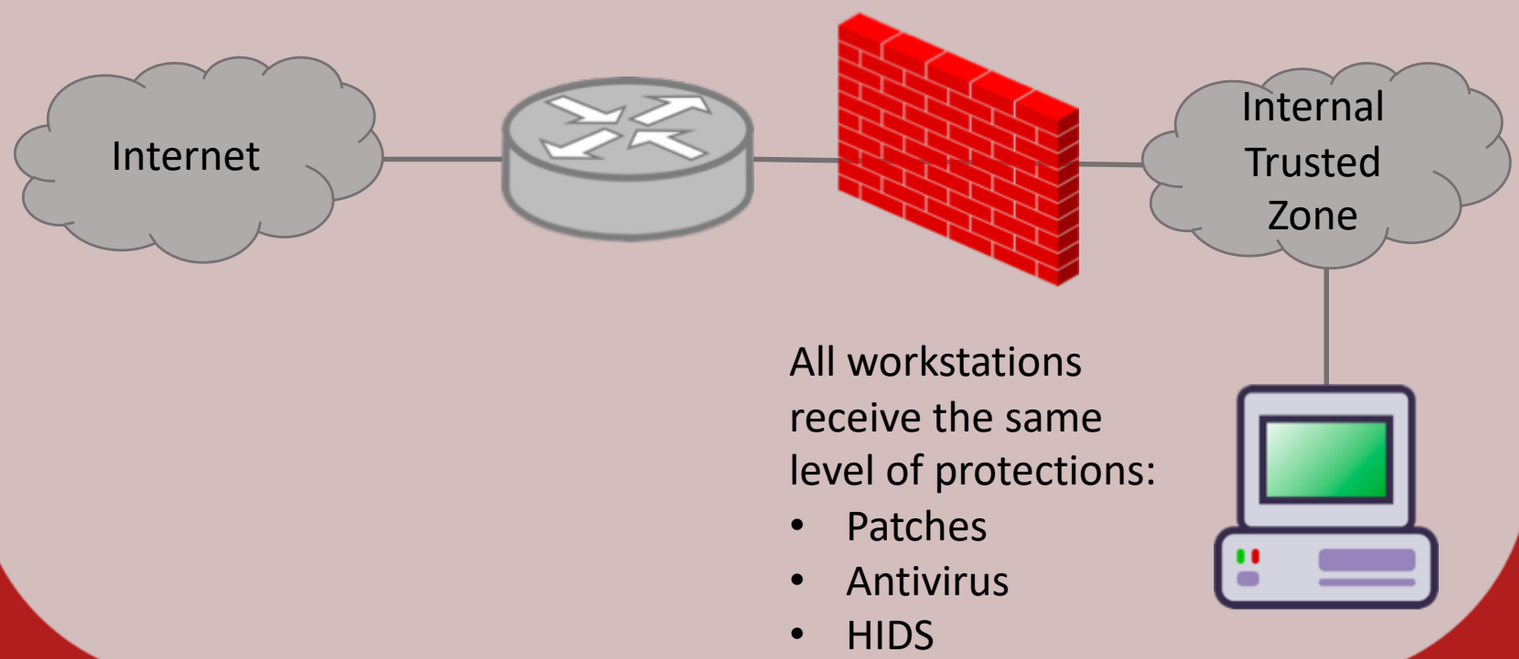
TRAINING THE CYBER SECURITY WORKFORCE

Layered Security Defense

- Difficult to design and implement
- Must consider business needs and usability in the design of layered controls
- Four design models
  - Uniform Protection
  - Protected Enclaves
  - Risk or Threat Analysis-based
  - Information Classification-based

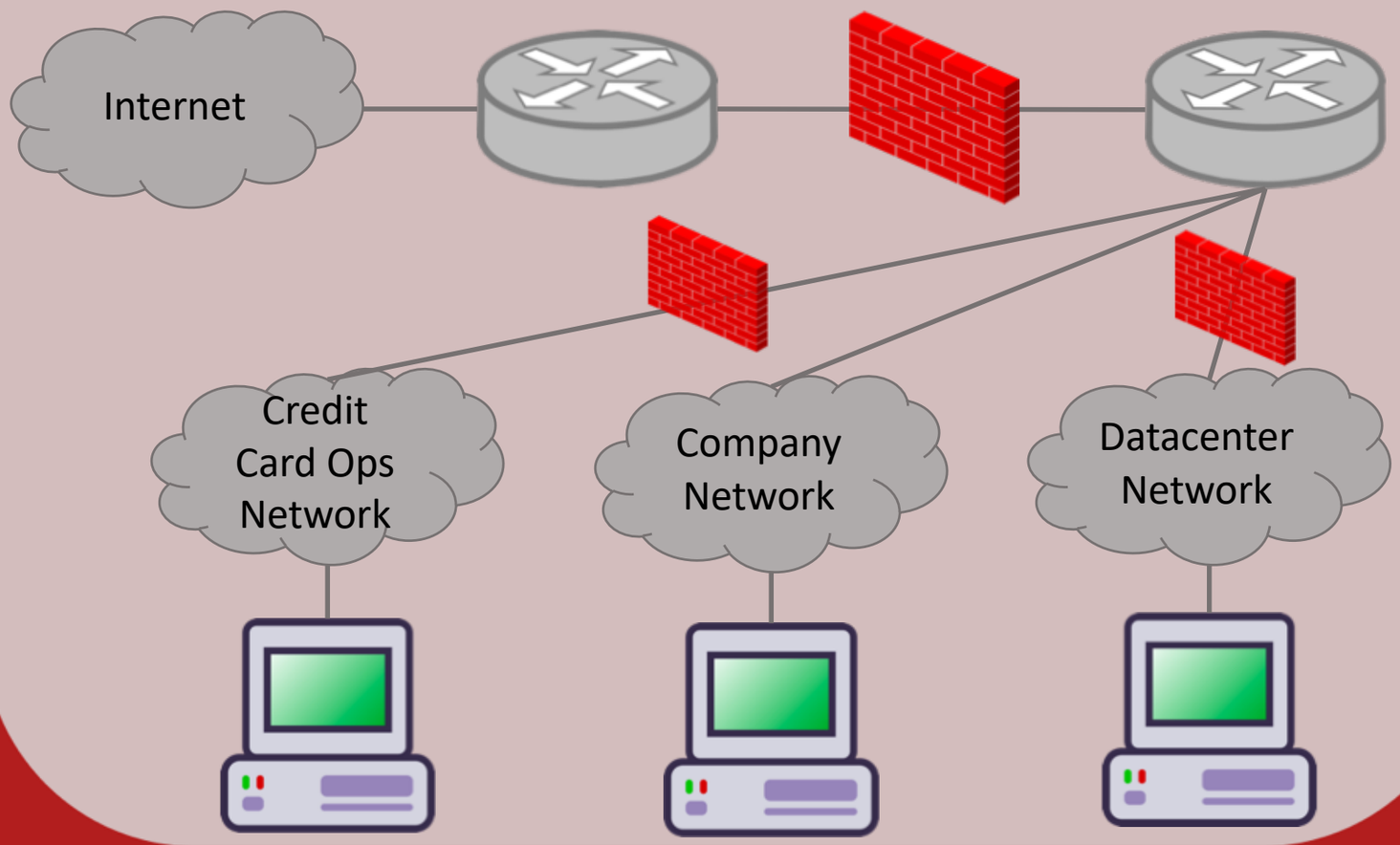
Uniform Protection

- Gives same level of protection to all data, systems, or networks
- Can be expensive for larger networks



Protected Enclave

- Enclaves that house more sensitive data are given additional protections



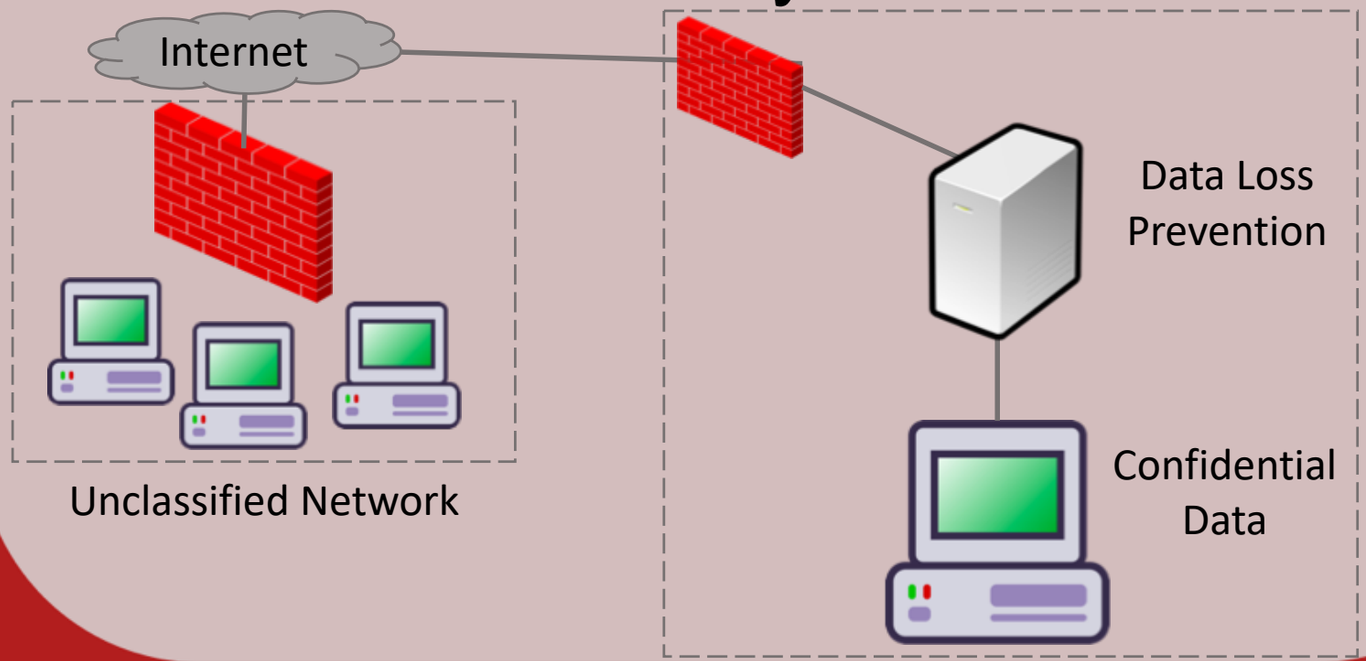
Risk or Threat Analysis-based

- Addresses specific risks or threats in the design of the networks and systems

- Example
  - If you are concerned with phishing as a threat vector, you could employ additional controls to securely scan and filter your incoming emails

Information or Classification-based

- Map data protection to different classes of information
- Higher classification levels get additional attention and security controls



JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Combining Design Models

- Often, these four models are combined as opposed to picking a single model