SECURITY POLICY

SECURITY ARCHITECTURE

© 2008 Security Architecture - All Rights Reserved.

CONTENTS

- Why a Course on Policy?
- Information Security Policy
- Policy in Context
- Regulatory Drivers
- Policy Standards
- Policy Development
- Writing Policies and Guidelines
- ... and Summary

© 2008 Security Architecture - All Rights Reserved.

SECTION 1: WHY POLICY?

WHY POLICY?

- Policy is the foundation for all the other elements in information security.
- Without effective policies there is no basis for ensuring that security tools, technologies, and processes are used appropriately to address risks.

© 2008 Security Architecture - All Rights Reserved.

WHY POLICY?

- Developing policy is an art, always specific to the organization in question.
- No one can sell you pre-written policies.
- There are processes, templates, and good information sources that can help.

© 2008 Security Architecture - All Rights Reserved.

WHY POLICY?

- Security in many organizations today is too focused on technology and tools, and not enough on business requirements, physical and information assets, and risk assessment.

© 2008 Security Architecture - All Rights Reserved.

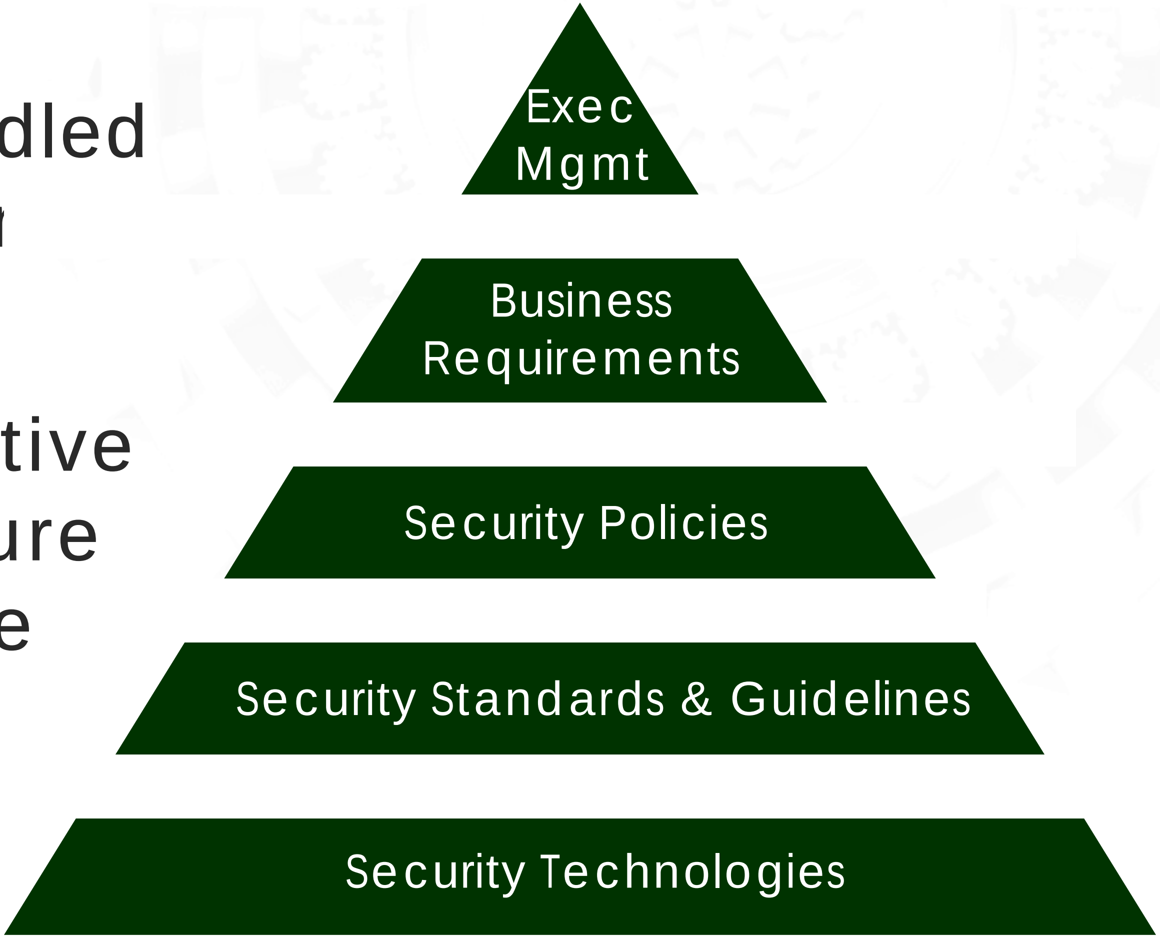
WHY POLICY?

- Policy addresses all elements of security in your organization:
  - People
  - Communications
  - Processes and operations
  - Physical and intellectual property
  - Technical infrastructure

© 2008 Security Architecture - All Rights Reserved.

WHY POLICY?

- Security is commonly handled from the bottom up, but…
- The most effective security structure begins from the top down →



© 2008 Security Architecture - All Rights Reserved.

WHAT IS POLICY?

- Security policy is a set of documents that explain how an organization will protect its physical and electronic assets.

- Policy states what will (or will not) be done, how policy is to be carried out and enforced, and often why the policy exists.

© 2008 Security Architecture - All Rights Reserved.

WHAT IS POLICY?

- Security policy addresses:
- Employee behavior
- Business practices
- Risk management
- Operations
- Technical measures

© 2008 Security Architecture - All Rights Reserved.

EMPLOYEE BEHAVIOR

- Acceptable use policy
- Email and communications policy
- Security awareness and education
- Access control policy
- Regulatory compliance
- Roles and responsibilities

© 2008 Security Architecture - All Rights Reserved.

BUSINESS PRACTICES

- Acceptable use policy
- External communications policy
- Transaction security policy
- Privacy policy
- Change management
- Security planning
- Regulatory compliance

© 2008 Security Architecture - All Rights Reserved.

RISK MANAGEMENT

- Business asset valuation
- Risk acceptance policy
- Mission Impact Assessment
- Disaster recovery/business continuity policy
- Internal controls
- Audit and assessment policy

© 2008 Security Architecture - All Rights Reserved.

OPERATIONS

- Acceptable use policy
- Email and communications policy
- Network and security monitoring
- Incident response
- Access control policy
- Physical security

© 2008 Security Architecture - All Rights Reserved.

TECHNICAL MEASURES

- Anti-virus policy
- Firewall policy
- Intrusion detection policy
- Application security policy
- Identity management and provisioning
- Access control
- Fraud detection

© 2008 Security Architecture - All Rights Reserved.

DEFENSE IN DEPTH

- Is the practice of layering defenses to improve an organization's security posture.
- Is a leading security principle in information assurance.
- Applies to any or all layers in a security architecture.

© 2008 Security Architecture - All Rights Reserved.

DEFENSE IN DEPTH

Defense in depth is an integrated set of information security measures and actions, implemented to provide multiple layers of security across:

- People
- Technology
- Operations

© 2008 Security Architecture - All Rights Reserved.

People

- Information security begins with commitment from senior management
- Policies and procedures should cover all organizational aspects related to people
  - Training and awareness
  - Personnel security
  - Human resources
  - Physical security

© 2008 Security Architecture - All Rights Reserved.

DEFENSE IN DEPTH

Technology

- Security measures should be deployed at network, platform, and application layers
- Security technology should be chosen to address stated policies based on identified risks
- Technology is a means to implement security policy

© 2008 Security Architecture - All Rights Reserved.

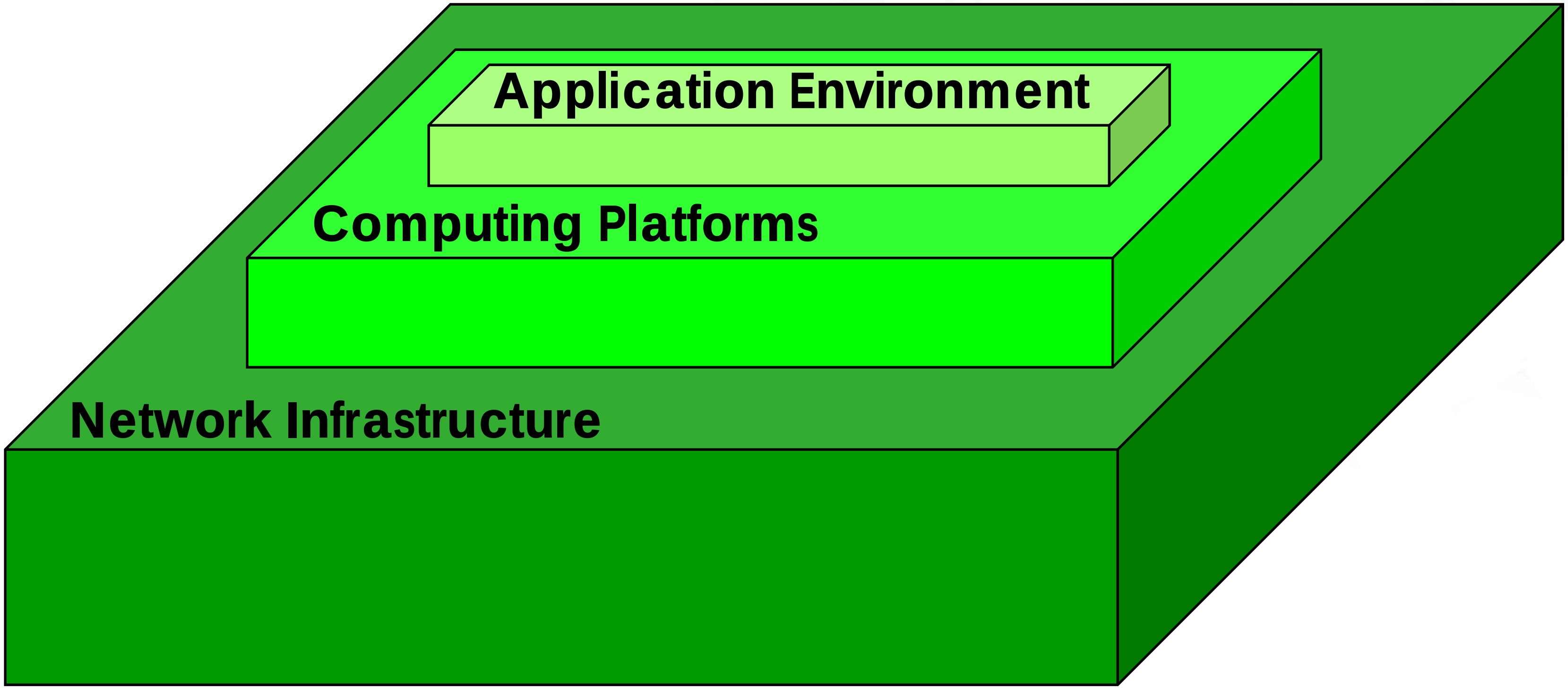
Operations

- Day-to-day activities to maintain security posture:
  - Security management
  - Monitoring and event management
  - Readiness assessments and testing
  - Certification and accreditation
  - Intrusion detection, alerting, and response
  - Patch management
  - Training

© 2008 Security Architecture - All Rights Reserved.

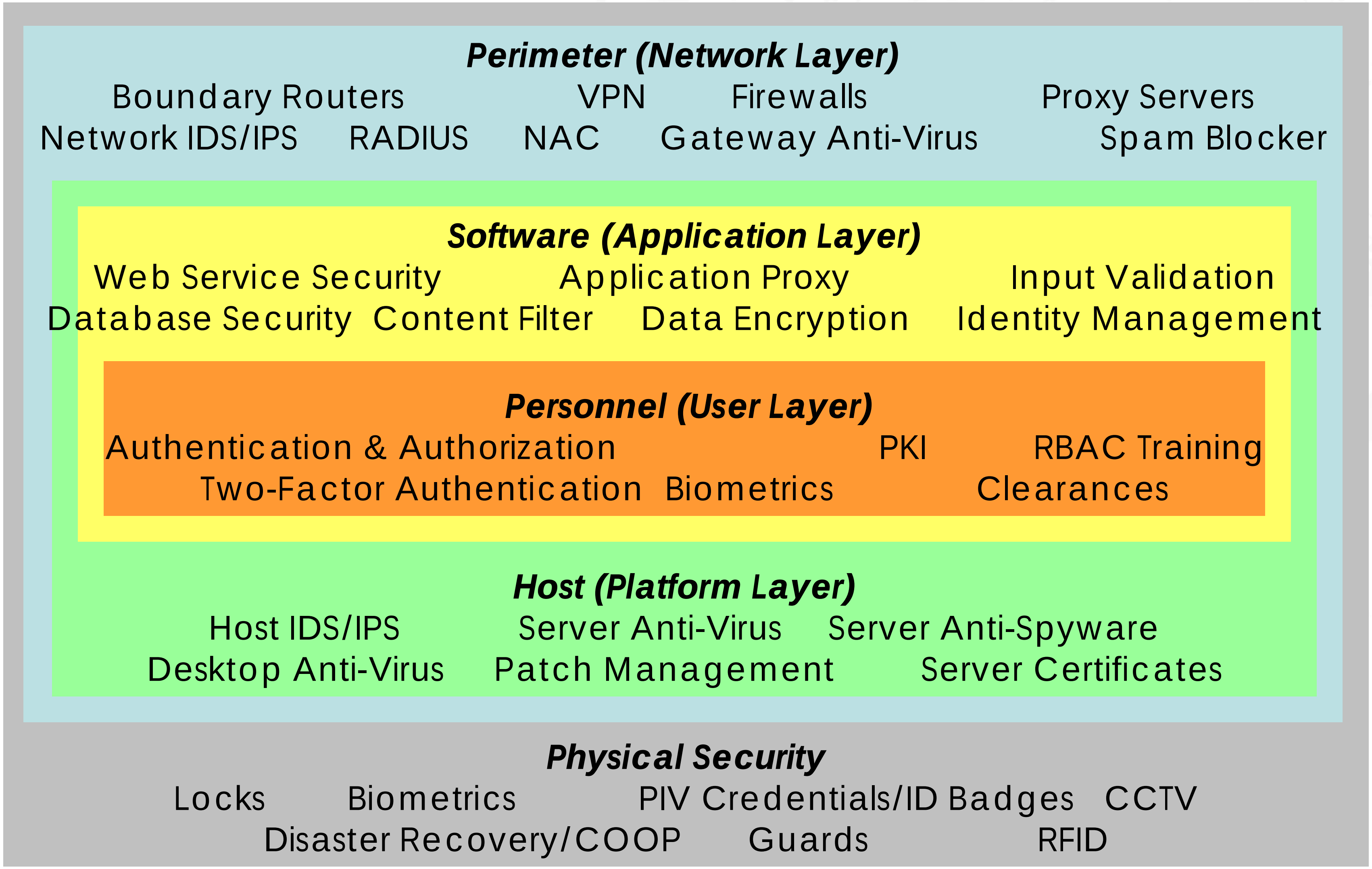
DEFENSE IN DEPTH

Security layers form a concentric set of boundaries:



© 2008 Security Architecture - All Rights Reserved.

DEFENSE IN DEPTH



Perimeter (Network Layer)

Boundary Routers VPN Firewalls Proxy Servers
Network IDS/IPS RADIUS NAC Gateway Anti-Virus Spam Blocker

Software (Application Layer)

Web Service Security Application Proxy Input Validation
Database Security Content Filter Data Encryption Identity Management

Personnel (User Layer)

Authentication & Authorization PKI RBAC Training
Two-Factor Authentication Biometrics Clearances

Host (Platform Layer)

Host IDS/IPS Server Anti-Virus Server Anti-Spyware
Desktop Anti-Virus Patch Management Server Certificates

Physical Security

Locks Biometrics PIV Credentials/ID Badges CCTV
Disaster Recovery/COOP Guards RFID

© 2008 Security Architecture - All Rights Reserved.

LEADING INFOSEC INVESTMENTS

- Network Security
  - Distributed security controls
  - Policy and configuration enforcement (NAC)
  - Event monitoring and management (SIEM)
- User Management
  - User provisioning/identity management
  - Single sign-on
- Content Security
  - Anti-virus/anti-spyware
  - Content filtering and spam control
  - Data loss protection

© 2008 Security Architecture - All Rights Reserved.