Protecting Information Assets
- Week 11 -

Application Development Security

MIS5206 Week 11

- Team Presnetations
- Readings
- Application Development Security
- Test Taking Tip
- Quiz

Reading

- Vacca Chapter 33, 34
- “In the News” article
- Case 2 – Prepare Analysis: SECURITY BREACH AT TJX
- SANS Assignments 4, 5

Application Development Security

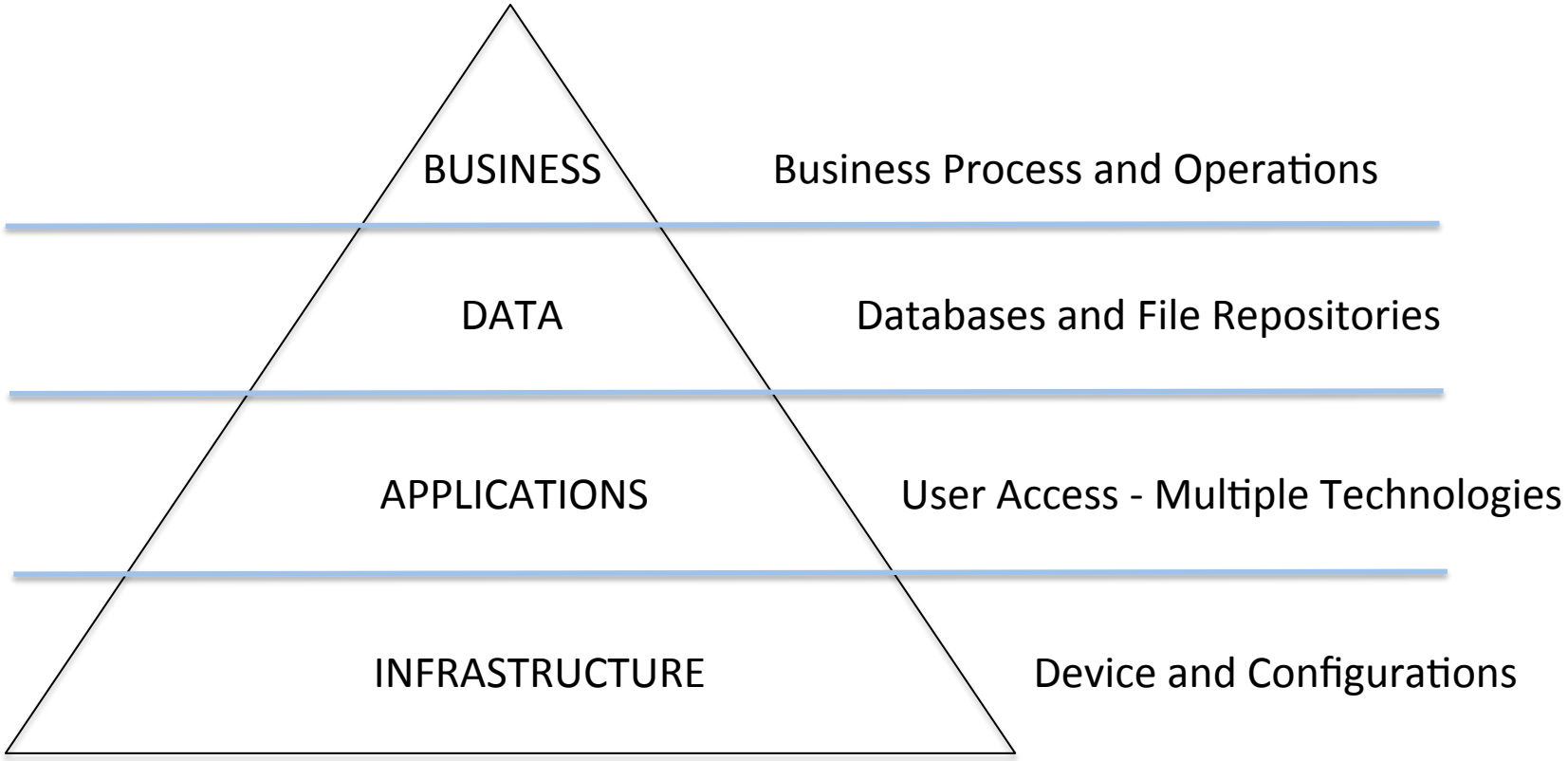
As applications become more accessible though the web, cloud and mobile devices, companies are being forced to abandon their reactive approach to security and, instead, to take a proactive approach by minimizing risk directly in the software they buy and create to serve their customers.

Best Practice: Build Security In

Security Architecture	Creation of, communications of and enforcement of System Architecture standards provides the basic building blocks for developing, implementing and maintaining secure application
Systems Development Life Cycle	Attention to security throughout the Systems Development Lifecycle is the key to creating secure, manageable applications regardless of platform or technologies
Procurement Standards	Describing the process and detailed criteria that will be used assess the security level of third party software enables companies to make strategic, security-sensitive decisions about software purchases

Security Architecture

Security strategy needs to be a consideration at each level of the architecture



Security System Development Lifecycle

- Phase 1: Initiation
- Phase 2: Development/Acquisition
- Phase 3: Implementation
- Phase 4: Operations/Maintenance
- Phase 5: Disposal

Phase 1: Initiation

- Data Sensitivity Assessment
- Preliminary Risk Assessment (RA)
- Review Solicitations (e.g. Request for Proposals - RFPs)

Phase 2: Development/Acquisition

- Functional and Technical Features/ Requirements
- Staff background Checks
- Operational Practices
- Test Plans, Scripts, and Scenarios
- Security Controls in Specifications

Phase 2: Development/Acquisition

In-House Concerns:

- Security features
- Development process
- Changing requirements
- Threats
- Vulnerabilities
- Malicious insiders

Phase 2: Development/Acquisition

- COTS Applications
- Operational Practices
  - System Security Plan (SSP)
  - Contingency Plan (BCP/DRP)
  - Awareness
  - Training
  - Documentation

Phase 3: Implementation

- Testing and Accreditation
  - Test Data
  - Test unit, subsystem, and entire system
  - Technical evaluation
- Security Management - administrative controls and safeguards

Phase 3: Implementation

- Physical facilities
- Personnel, responsibilities, job functions, and interfaces
- Procedures (e.g. backup, labeling)
- Use of commercial or in-house services

Phase 3: Implementation

- Disaster Recovery Plan (DRP)
- COTS products (security patches?)
- Remove installation programs
- Machine content/intent
- File and program overlay settings and privileges

Phase 3: Implementation

- Backup, restore, and restart instructions and procedures
- Implementation backups (could server as benchmark)
- Ensure implementation of only approved/accredited systems

Phase 4: Operations/Maintenance

- Backup and restoration parameters
- Performing backups
- Support training classes
- Cryptography keys
- User administration and access privileges
- Audit logs

Phase 4: Operations/Maintenance

- Log file analysis
- Security software
- Physical protection
- Off-site storage
- Output distribution
- Software & hardware warrantees
- Registration/Deregistration

Phase 4: Operations/Maintenance

- Operational Assurance Activities:
  - Review runtime operation
  - Review technical controls
  - Verify documentation of access permissions
  - Review system interdependencies
  - Verify that documentation is current
  - Verify proper use of deregistration
  - Verify that documentation is accurate

Phase 5: Disposal

- Storage of cryptographic keys
- Legal requirements of records retention
- Archiving federal information
- Sanitize media

Procurement Security Considerations

Differ based on type of procurement

- Software purchase
  - Commercial Off-The-Shelf (COTS)
  - Custom development
- Outsourcing of services
  - Not just software
- Software as a service
  - e.g. Online Tax Services

COTS Software

- Clout is key
  - Big markets: U.S. Government?
- Security requirements definition in RFP is important
  - Possible product differentiator
- Contract security language
  - Growing importance and emphasis
- Major vendors starting to “see the light”

Custom Software

- Software security and vendor requirements need to be specific and detailed
- Education may be necessary
- Possible vendor differentiator
- Ongoing patching and support is important

Outsourcing

- Services and hosting as well as software
- Define security goals and policies
- Ensure outsourcing maintains the same level of compliance
- Beware of sub-outsourcing

Software as a service

- Who controls the data?
- Is security adequate for all types of data?
  - Map to data classification
- Ensure service maintains compliance with policies and security goals
- Don't forget e-Discovery

Test Taking Tip

Focus on addressing each question individually

- As you take the test, if you don't know an answer, don't obsess over it
- Answer the best way you can or skip over the question and come back to it after you've answered other questions

Quiz