ISE West Executive Forum and Awards

Nominee Showcase Presentation

September 16, 2010

Company Name:	McKesson Corporation
Project Name:	Application Security Risk Management
Presenter:	John B. Sapp Jr. – CISSP, CGEIT, HISP
Presenter Title:	Director, Product Development Standards – Security, Risk & Compliance

T.E.N.
TECH EXEC NETWORKS

Company Overview

- **Oldest Healthcare Services Company (1833) and Largest Healthcare IT vendor**
  - *Software & Hardware technology installed in 70% of U.S. hospitals with more than 200 beds*
- **14th in Fortune 500 – FY10 Revenue: $108B**
- **34,000+ employees (Global)**
- **360-degree view of healthcare**
  - *200,000 physicians*
  - *26,000 retail pharmacies*
  - *10,000 extended care facilities*
  - *5,000 hospitals*
  - *2,000 medical-surgical manufacturers*
  - *750 homecare facilities*
  - *600 health care payors*
  - *450 pharmaceutical manufacturers*

T.E.N. TECH EXEC NETWORKS

McKESSON

Empowering Healthcare

360-degree view of Healthcare

Presentation/Project Overview

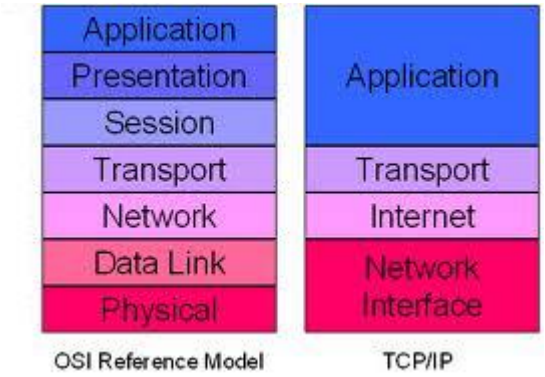
- Visionary Leadership
- Application Software: “The New Perimeter”
- Goals and Objectives
- Application Security Risk Management
- Application Security Maturity Model

Visionary Leadership

- Executive Sponsors
  - Sharen Bond, VP Development Support Services
    Office of the CTO
  - Michael Wilson, VP CISO
    Office of the CTO
  - Randy Spratt, EVP CIO & CTO

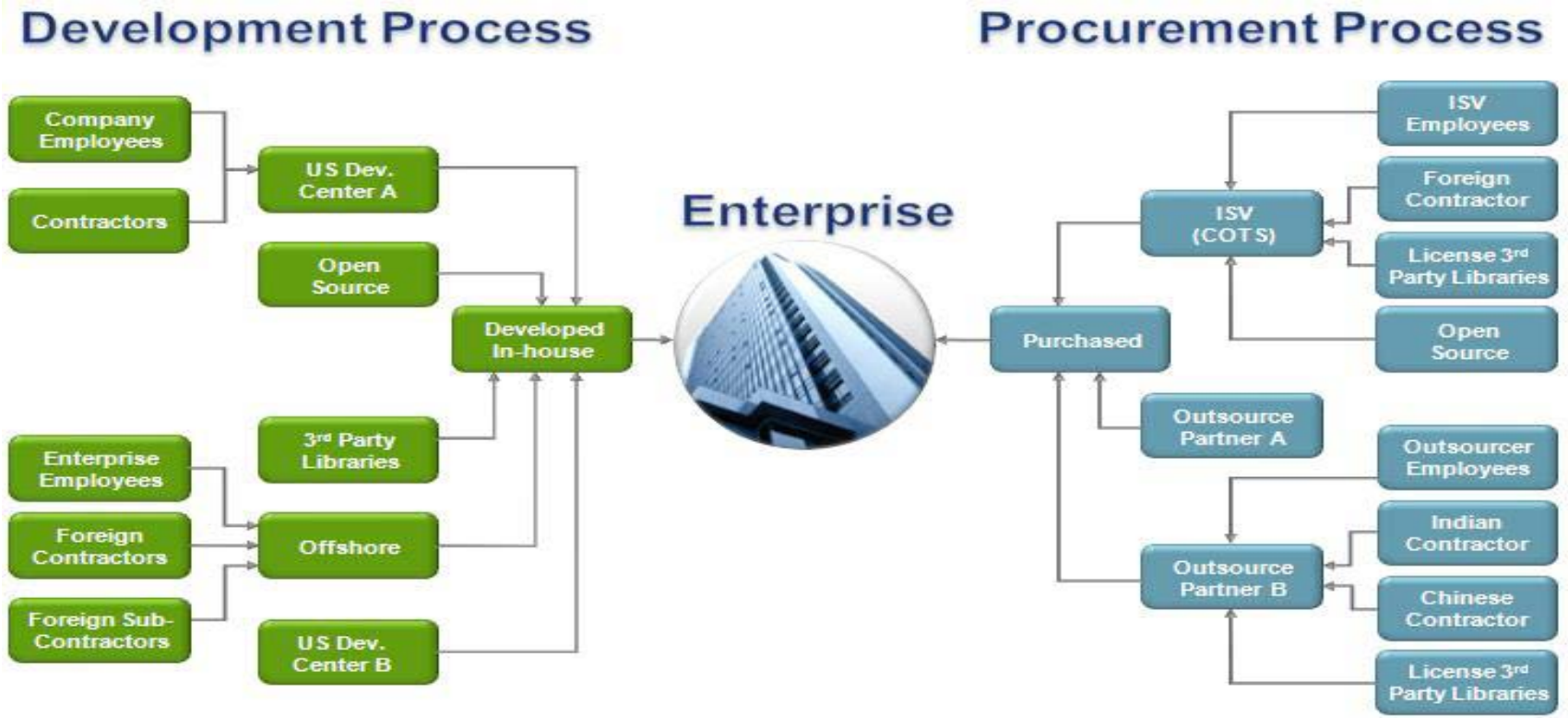
Overview of Business Challenge

- Application Software (Layer 7)
  - Least defended layer of OSI-stack
  - Source for 95% of Reported Vulnerabilities [1]
  - Target for 75% of Attacks[2]
- SOUP – Software of Unknown Pedigree



[1] Mark Curphey, "**Software Security Testing: Let's Get Back to Basics**" – October, 2004, SoftwareMAG.com
[2] Theresa Lanowitz, "**Now Is the Time for Security at the Application Level**" – December 2005, Gartner
Dr. Dobbs - Making Sense of Software of Unknown Pedigree

Overview of Business Challenge

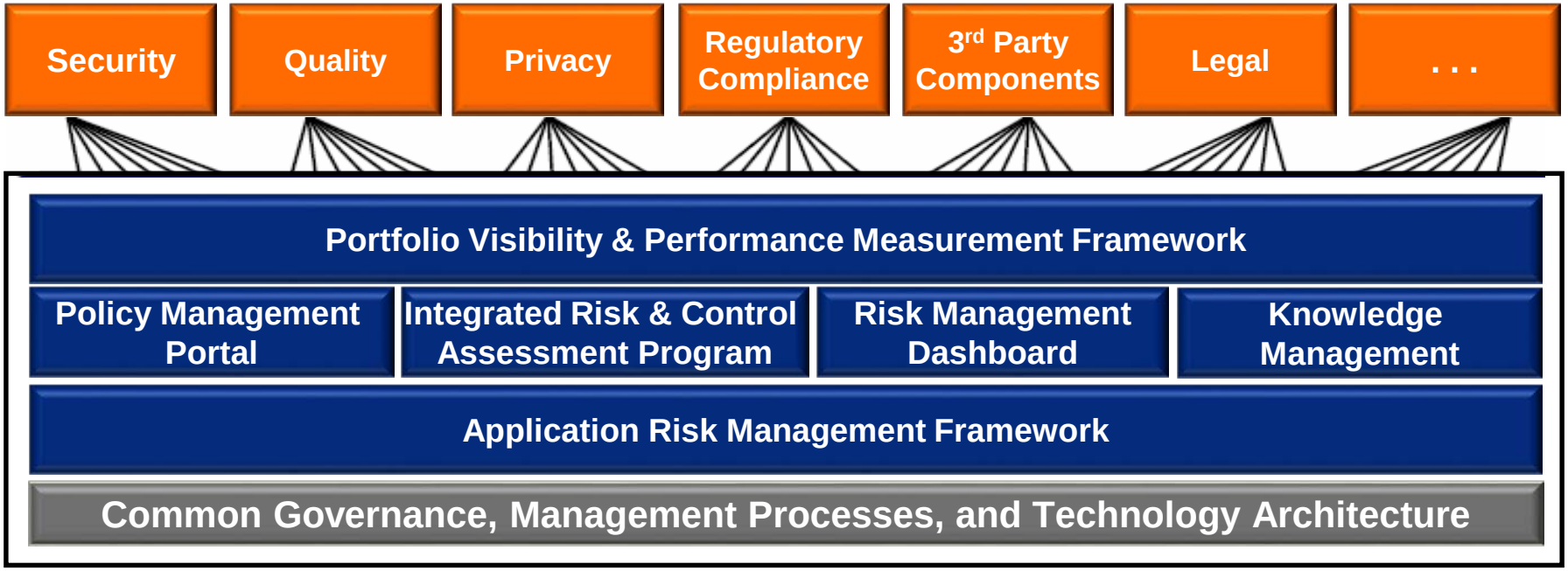


Program Scope/Goals

- Enterprise-wide Application Development
  - Software Products developed for healthcare market
  - Applications leveraged for operational support
- Goals and Objectives
  - Optimize Investments through a harmonized program
  - Establish Application Risk Management Process
  - Formalize Application Portfolio Governance
  - Increase Transparency and Visibility

PRiME Program

Product Risk Management for the Enterprise



Program Results

- Purpose-built framework for managing Application Risk across multiple risk domains
- Successfully completed static / dynamic analysis and established remediation plans for numerous McKesson software products in preparation for HITECH certification

Lessons Learned/Best Practices

- Cultural change is evolutionary and the key to long-term success
- It's about RISK, not just security vulnerabilities
- Static binary analysis yields critical information not available with static source analysis
- Tools and technology enable a repeatable and sustainable process, but are not the focal point

Thank you and Questions

- Questions?