Update Management for Control Systems

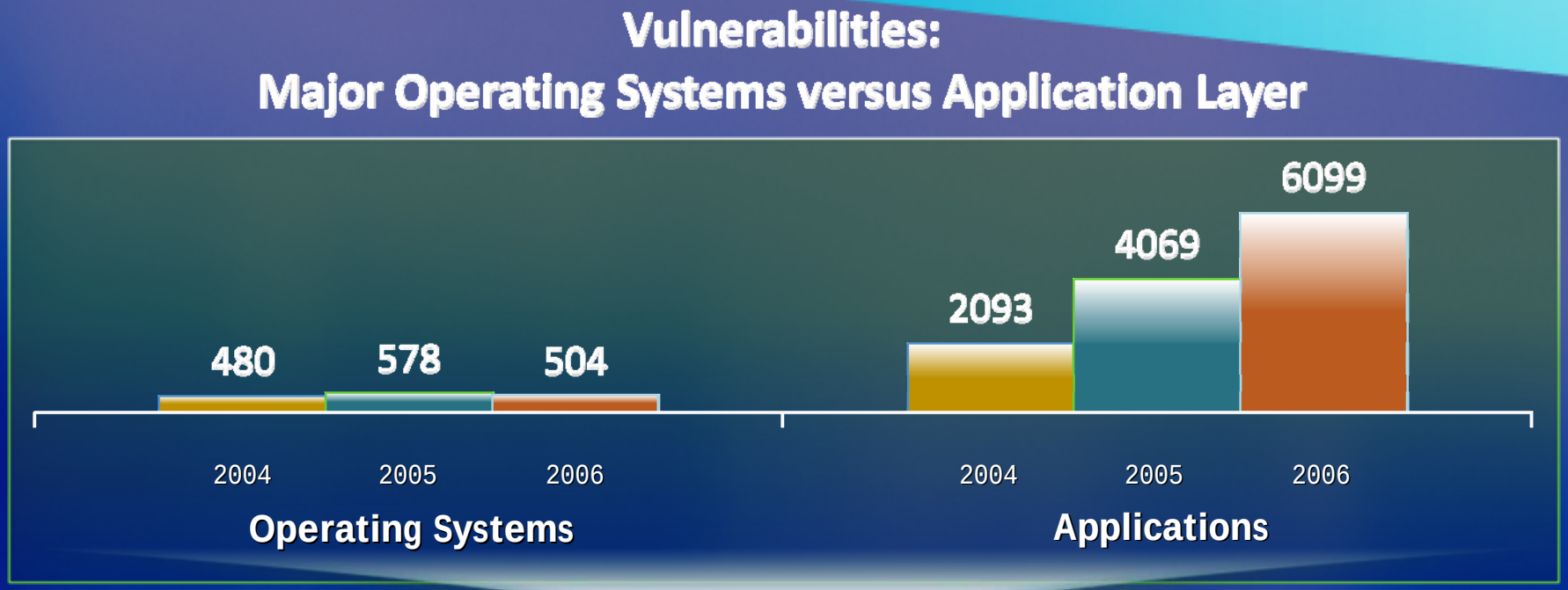
Kevin Sullivan
Sr. Security Strategist
Microsoft

Microsoft
Critical Infrastructure Protection

Common Security Challenges

- Ubiquitous connectivity
- Use of commodity software
- Fast growing deployed base
- Focus of attackers
- Media coverage

Application Layer Attacks



Source: Microsoft Security Intelligence Report 2007

~90% are remotely exploitable

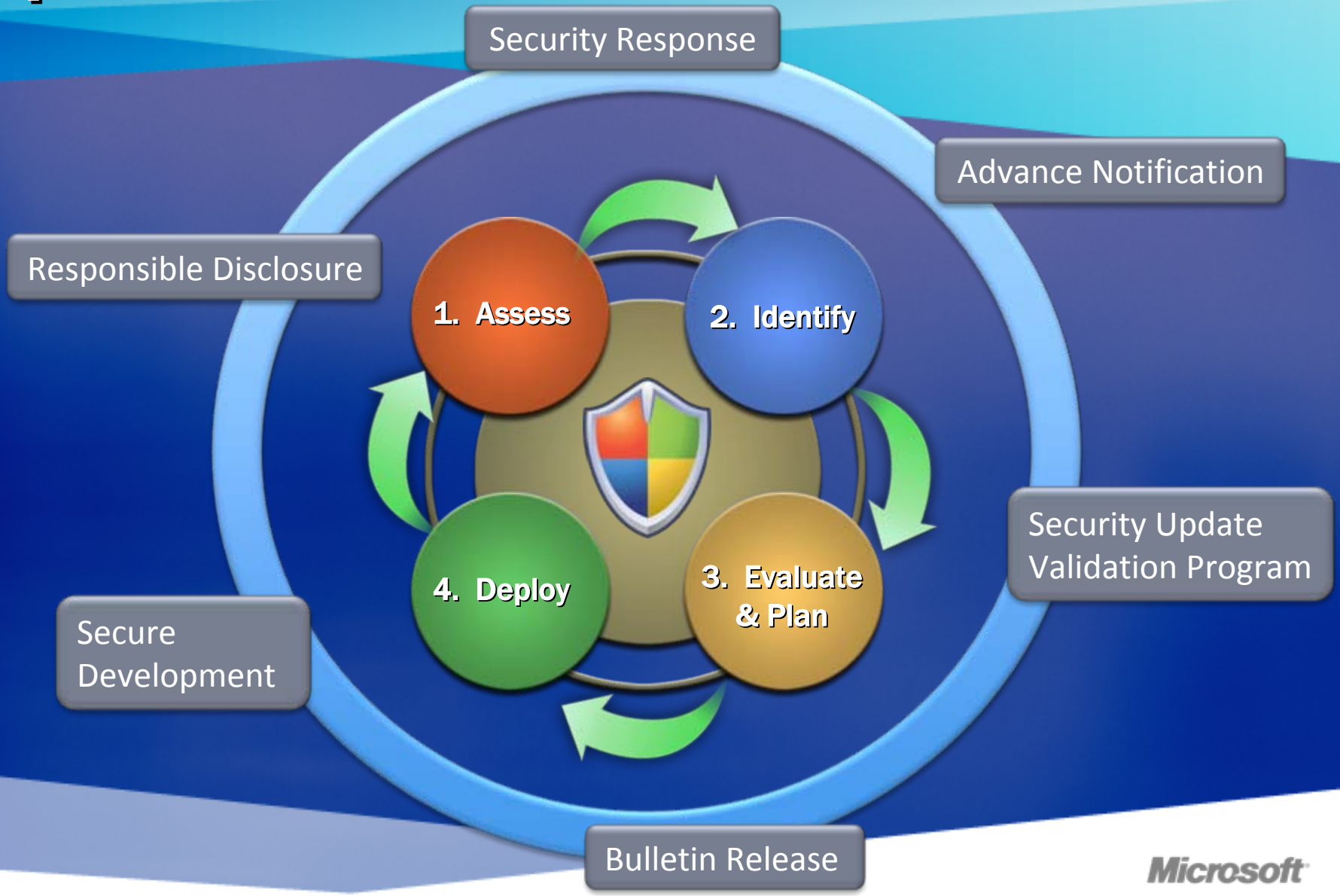
~60% are in web applications

Update Philosophy

- Plan for updates to the entire infrastructure stack:
  - Network
  - Operating System
  - Database
  - Application
- Architect your systems for updates:
  - Redundancy
  - Virtualization

Updates should be manageable and predictable.

Update Mechanics



Update Innovations

- Exploitability Index
  - 1 = Consistent Exploit Code Likely
  - 2 = Inconsistant Exploit Code Likely
  - 3 = Functioning Exploit Code Unlikely

Customer Goal:

Prioritize Updates

- Windows Server 2008 - Server Core
  - Reduced attack surface
  - Infrastructure roles only
  - Limited GUI

Customer Goal:

Fewer Updates

Microsoft®

Your potential. Our passion.™