

Update Management for Control Systems

Kevin Sullivan
Sr. Security Strategist
Microsoft

Common Security Challenges

Networked OS
1999

Control Systems
2009

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

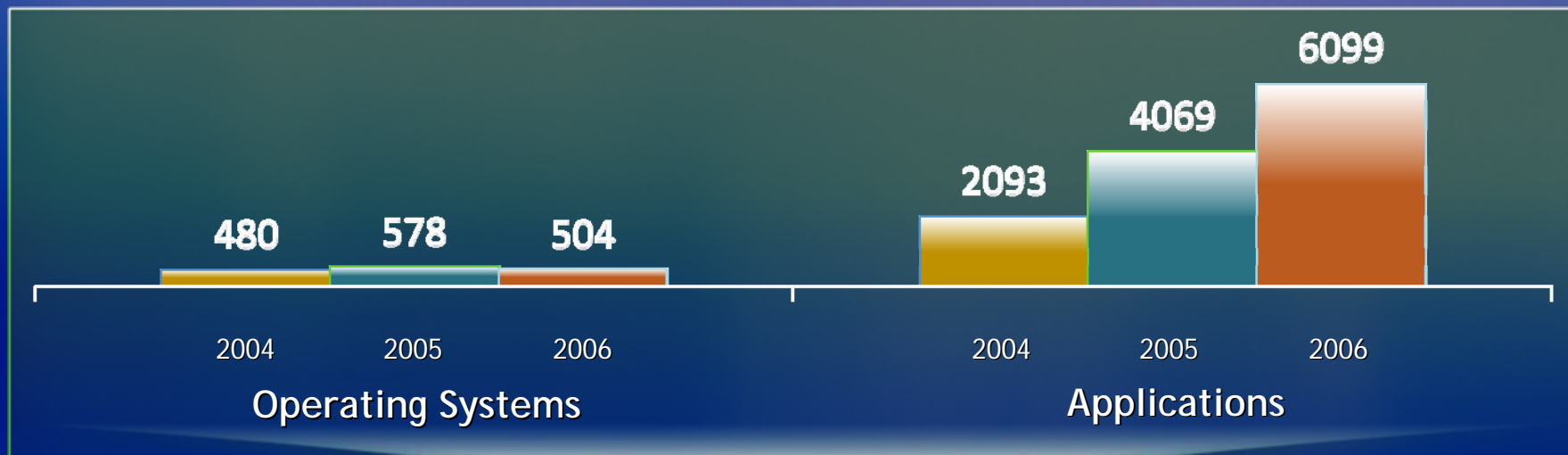


Microsoft

Critical Infrastructure Protection

Application Layer Attacks

Vulnerabilities: Major Operating Systems versus Application Layer



Source: Microsoft Security Intelligence Report 2007

~90% are remotely exploitable

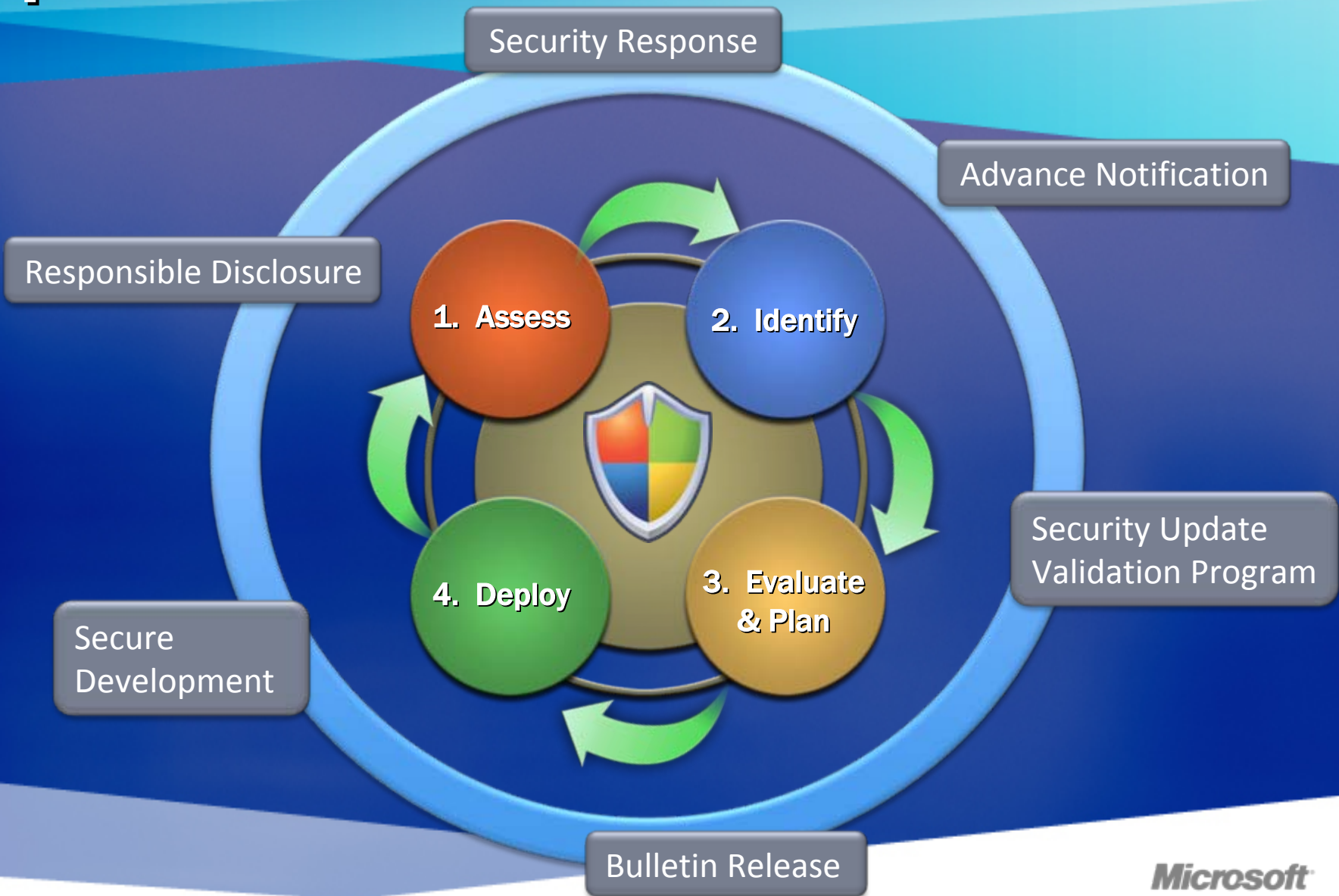
~60% are in web applications

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 = Inconsistent Exploit Code Likely
 - 3 = Functioning Exploit Code Unlikely

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

Customer Goal:

Prioritize Updates

Customer Goal:

Fewer Updates

Microsoft

Critical Infrastructure Protection

Microsoft[®]

Your potential. Our passion.[™]

© 2009 Microsoft Corporation. All rights reserved. Microsoft, Windows, Windows Vista and other product names are or may be registered trademarks and/or trademarks in the U.S. and/or other countries. The information herein is for informational purposes only and represents the current view of Microsoft Corporation as of the date of this presentation. Because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information provided after the date of this presentation.
MICROSOFT MAKES NO WARRANTIES, EXPRESS, IMPLIED OR STATUTORY, AS TO THE INFORMATION IN THIS PRESENTATION.