The Business Case for Checklist Development

Philip Reitinger
Senior Security Strategist
Trustworthy Computing Team
Microsoft Corporation

Security Must Be Easy

- The threat is increasing
  - Increasing reliance on systems
  - The Internet is an open system
  - Interdependence is rising
  - Computer literacy is on the rise among prospective attackers
  - Hacking and disruption are becoming easier in some ways – training and automated tools
- View of risk has changed
- A majority of computer are in unmanaged environments

Security Framework

SD³ + Communications

Secure by Design	• Secure architecture • Security aware features • Reduce vulnerabilities in the code
Secure by Default	• Reduce attack surface area • Unused features off by default • Only require minimum privilege
Secure in Deployment	• Protect, detect, defend, recover, manage • Process: How to's, architecture guides • People: Training
Communications	• Clear security commitment • Full member of the security community • Microsoft Security Response Center

Secure in Deployment

- Training
- Create deployment and security tools
- Make the process easier
  - Automate where possible
  - Microsoft Security Response Center
- Configuration
  - Design for ease of or auto-configuration
  - Provide configuration guidance to administrators and users

Checklists

- The majority of attacks can be stopped or mitigated by appropriate configuration
- Checklists make the process of configuration much easier in managed or unmanaged environments

Checklists – Vendor Development Advantages

- Knowledge of product
- Significant testing resources
- Responds to customer demand
- May be required for product certification
  - E.g., a Common Criteria PP which requires a locked-down configuration
- Leads to enhanced support

Vendor Development Advantages, Continued

- Vendors can coordinate with multiple parties to:
  - Ensure a broad range of criteria are met, including through guidance for multiple levels
  - Balance usability and security

Microsoft Examples

- Have shipped guides for locking down Windows systems with scripts for automated application
  - Multiple guides that can be applied depending on the environment
- Checklists
- Available at www.microsoft.com/technet/security

Vendor Development Disadvantages

- Cost
- Trust

Third-Party Checklists

- There is no one-size-fits-all solution
- Microsoft supports third-party efforts to develop guidance for particular environments
- Consistency among checklists for similar environments is important
  - Microsoft continues work with CIS, NIST, SANS, NSA, and DISA to enhance and converge guidance
- “We agree” helps validate vendor and third-party guidance


Microsoft®
© 2003 Microsoft Corporation. All rights reserved.
This presentation is for informational purposes only. Microsoft makes no warranties, express or implied, in this summary.