THE SECURITY STANDARD™

Securing the Enterprise from a Dangerous Cyberworld

September 19-20, 2011 • Marriott Brooklyn Bridge, New York City

Produced by
CSO

How to Align Appropriate Security Across More Devices

Lee Parrish

CISO

Parsons

Lee Parrish – VP & CISO, Parsons Corp

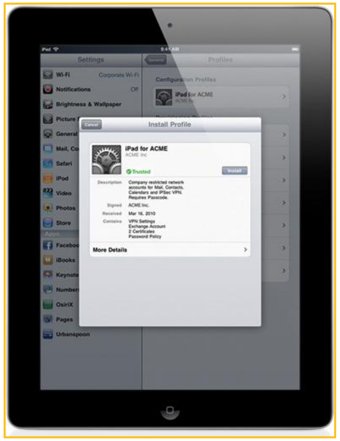
Parsons, celebrating more than 65 years of growth in the engineering and construction industry, is a leader in many diversified markets with a focus on infrastructure, environmental, and defense/security. Parsons delivers design/design-build, program and construction management, professional services, and innovative alternative delivery solutions to federal, regional, and local government agencies worldwide, as well as to private industrial customers. For more about Parsons, please visit www.parsons.com.

Mobile Platform Evolution

- 1st gen cell phone - wide use of cell phones - smart phones/tablets
- How do we look upon these devices?
  - Supplement to computer?
  - The computer?
- Vulnerabilities/Malware Increases on Mobile Devices
  - Types of vulnerabilities in Apple iOS 2007-2010 - vulnerabilities, not exploits (source: Gartner)
  - 76% jump in malware targeting Android in Q2 2011 (source: McAfee)
  - Popularity + Increased Level of Data = Target for malware

Applying Security

- To address mobile security effectively, our organizations need to focus on three key areas:
  - Policy
  - Technology
  - People



Install Profile

iPad for ACME
ACME Inc
Trusted

Description: Company restricted network accounts for Mail, Contacts, Calendars and IPSec VPN. Requires Passcode.
Signed: ACME Inc.
Received: Mar 16, 2010
Contains: VPN Settings
Exchange Account
2 Certificates
Password Policy

More Details

POLICY

Policy Considerations

- What will you allow on your corporate network?
  - Core list of standards
  - BYOD
- The business should drive technology, and not vice versa
- Does each employee require a desktop + laptop + iPad + smart phone?
- If you do allow personal devices that are corporate managed, consider an Employee User Agreement:
  - Information Security has the authority to remotely wipe corporate data on personal devices (and personal data if necessary) should the need arise.
  - Statements of liability; ensure employees back up regularly

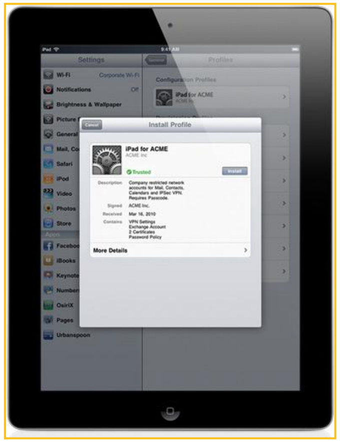
Mobile Device Policy

- No ‘jailbreak’ policy
- All security requirements
  - Password length, changes, failed attempts, etc.
  - When user separates from the company
  - Must participate in Mobile Device Management program
- Minimum device level
  - iPhone 3GS + iOS 4.2 or higher; new install
- Only allow closed app development?
  - Ex: Apple Application Provenance
  - Doesn’t solve the issue but adds another layer of protection

Processes/Procedures

- With new security controls, ensure that there are processes for them:
  - Wiping data
  - Remote lock
  - Reporting stolen devices and next steps
  - Terminated employees
  - Etc.

TECHNOLOGY



Install Profile

iPad for ACME
ACME Inc

Trusted

Description: Company restricted network accounts for Mail, Contacts, Calendars and IPSec VPN. Requires Passcode.

Signed: ACME Inc.

Received: Mar 16, 2010

Contains: VPN Settings
Exchange Account
2 Certificates
Password Policy

More Details

Central Management Solution

- Active Sync or…
- Mobile Device Management
  - Enforces alpha/numeric passwords (even across AD groups, Fed BU's)
  - Forces encryption native to the device
  - Authentication
  - Application control
  - Kicks jailbroken phones off the enrollment
  - Remote lock
  - Data wipe/selective wipe
  - If the profile is removed, locks out the user
  - Hardware inventory, reporting, can list recommended apps
  - Centrally managed

Other Technology Considerations

- Do you have forensic capabilities for mobile devices?
  - In house vs. outsourced
- How do we handle contractors and multi-user environments?

PEOPLE

Employee Considerations

- Self-Enroll Capabilities
  - Craft multiple installation guides that are easy to follow
- Communicate the mobile device policy
  - Explain the risks
  - Detail the controls in place and how they allow for mobile devices, even at a small inconvenience price.
- End User Agreement form
- Awareness articles
  - Build the demand prior to launching your mobile security controls
- Executive video awareness

ONE MORE THING…

Cultural Deployment

- Consider pilots and test programs first.
- Implement production in phases
  - Foundational controls first
  - Application control second
- Start at the top
- Frown upon waivers
- Keep up with the mobile threats and demand remediation strategies from supplier partners

QUESTIONS?

lee.parrish@parsons.com

THE SECURITY STANDARD™

Securing the Enterprise from a Dangerous Cyberworld

September 19-20, 2011 • Marriott Brooklyn Bridge, New York City

Produced by
CSO