



**Millennia**  
SYSTEMS INC

# Enabling Staff with Secure Mobile Technology in an Increasingly Risky World

**Dan Campbell**

**March 27, 2012**

**[www.MillenniaSystems.com](http://www.MillenniaSystems.com)**

**301-841-7400**

# Mobility = Mission Critical

- Mobility is no longer a luxury, it's a necessity
- Organizations encouraging telecommuting, hoteling, working remotely
- Individuals are used to being constantly connected
- Cultural shift towards smart phones, tablets, wireless
- Staff prefer to select and use personal devices over GFE
- Organizations can reduce hardware, support and service contract costs by permitting and promoting a BYOD culture
- Borderless networking and constant connectivity are vital

***Capabilities are tempered by the need to ensure data integrity and transaction security***

# Constant Connectivity

- **Wireless**
- **Mobile Handhelds and Tablets**
- **Remote Access VPN**
- **Virtual Desktop Infrastructure**

***How often do you work “offline” now?***

# Wireless Best Practices

- Risk-based approach
  - Define requirements according to organizational risk tolerance
  - Prioritize risks and map to available resources
  - Deploy solutions that balance risk with capabilities
- Adhering to standards
  - Review NIST, DoD, vendor and other industry sources
  - Tailor guidelines according to the unique requirements and security posture of your organization

***There is no one size fits all. Risk is partially subjective and relative. Use your own judgment according to your environment.***

# Wireless Best Practices

- **Standards-based technology deployment**
  - FIPS approved hardware
  - 802.11i, EAP, WPA2-Enterprise authentication, AES-CCMP encryption
  - Machine and user authentication, certificates, NAC, SSO, 2FA
  - Tune signal strength to reduce leakage and limit access
  - Supplement wired network IDS/IPS with wireless IPS (WIPS)
- **Security**
  - Develop policies on access control, authentication, acceptable use, dual-connected laptops, ad hoc networks, public wifi hotspots
  - Perform continuous monitoring for security breaches, rogue APs, SSID spoofing, intrusion attempts, interference as DoS
  - Update security awareness training, policies and procedures

# Guidelines and Standards

- 800-48 *Guide to Securing Legacy IEEE 802.11 Wireless Networks*
- 800-53 *Recommended Security Controls for Federal Information Systems and Organizations*
- 800-94 *Guide to Intrusion Detection and Prevention Systems*
- 800-97 *Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11ie*
- 800-114 *User's Guide to Securing External Devices for Telework and Remote Access*
- 800-120 *Recommendation for EAP Methods Used in Wireless Network Access Authentication*
- DISA STIG - [Wireless Security Technical Implementation Guide \(v6r2\), 23 April 2010](#)
- DISA STIG - [Wireless LAN Security Framework \(v1r0\), Addendum to the Wireless Security Technical Implementation Guide, Draft, 10 February, 2005](#)
- [Wireless Communication Standard, 2008](#)

# Mobile Handhelds and Secure Messaging

- Review industry standards and best practices, e.g., DISA STIGs
  - Consider whether device is GFE / Corporate or personally-owned
  - Policies will need to be balanced if personally-owned
- Develop requirements and policies
  - Tailor guidelines to organization-specific risk tolerance
- Stay in the application “sandbox” to the extent possible
  - Prevent copying data or storing documents outside the application
  - Avoid mixing the enterprise and personal contact lists
  - Enforce password policies, complexity, expiration, lockout
- Ensure remote wipe capability for lost devices

# Mobile Handhelds and Secure Messaging

- **Increase security awareness**
  - Smartphones are like computers - vulnerable to worms and viruses
  - Staff must be cognizant that their “personal” device contains organizational data
  - Develop procedures for lost devices, notification and remote wipe
- **Staff may have to be flexible**
  - Abide by organization security requirements
  - May limit some aspects of smart phone capabilities
  - Prohibit the use rooted androids and jailbroken iPhones
    - Detect for rooted / jailbroken phones periodically and wipe data

# Guidelines and Standards

- DISA STIG [Good Windows Phone Hardening Guide](#)
- DISA STIG [Good Android Hardening Guide](#)
- DISA STIG [Good iOS Hardening Guide](#)
- 800-101 Guidelines on Cell Phone Forensics
- 800-121 Guide to Bluetooth Security
- 800-124 Guidelines on Cell Phone and PDA Security

***“Sandbox” philosophy may need to be flexible as staff increasingly use tablets with local applications to balance security and capabilities.***

# Remote Access VPN

- Previously was for occasional use
  - Off hours or weekends to check email or do timesheet
- Now a primary means of connecting to enterprise resources
  - Telecommuting, travel, hoteling
  - Access beyond email to most if not all enterprise applications
- Staff access enterprise resources anywhere
  - Home, hotels, coffee shops and other public hotspots
  - Staff expectation is for there to be little if any difference in network experience, performance and capabilities

***Remote access is an extension of the enterprise network***

# Virtual Desktop Infrastructure

- **VDI is emerging as a popular means for endpoint deployment**
  - Replacing laptops and traditional desktop computers
  - Reduce hardware, licensing and support cost
  - Ease operation - images, troubleshooting, policy changes
  - Improve security by reducing endpoint intelligence
- **Constant connectivity is required for a successful VDI deployment**
  - Off-net capabilities limited
  - Network access to enterprise resources is now critical just for basic device functionality
- **Network performance is even more vital**

# Takeaways

- **Mobility = Mission Critical**
- **Staff require flexibility**
- **Being offline is rare - constant connectivity is vital**
- **Mobile solutions are virtual extensions of physical networks**
- **Deploy mobile solutions using a risk-based approach**
- **No “one size fits all” guideline for risk assessment**
- **Define solutions according to organizationally-specific criteria**
- **Security and capabilities must coexist and find balance**

# Action Items

- Review wireless security policies and risk mitigation strategies
- Compare your deployment with industry best practices from a variety of sources
- Review training plans and increase security awareness to ensure staff are cognizant of risks
- Perform continuous monitoring and constantly look to improve service and security through tools and procedures
- Conduct periodic reviews of policies, procedures and designs against changes to standards, technology or threats

***Never sit still. Stay mobile!***



**Millennia**  

---

**S Y S T E M S I N C**

**Realize Tomorrow. Today.**