!! Are we under attack !!

Personal Consumer devices continue to invade
Corporate enterprise – just wanting to plug in

Mobile Device Management

Overview

How It Got Here

- The main devices for corporate productivity used to be the desktop or laptop computer.
- RIM's BlackBerry opened the door for smartphones as business tools.
- Employees began bringing their own non-BlackBerry devices into work, and demanding that they be able to connect them with corporate resources

Where It's Going

- Mobile device management as a hub for managing a variety of corporate and personal
- Security is a focus of most MDM vendors.
- Mobile devices are increasingly application platforms.
- Mobile technology will continue to change rapidly

We must continue to focus on solutions that offer us Enforced Passwords, Device Wipe, Remote Lock, Audit trail/logging, Jailbreak detection, Software Distribution with Application downloading, updating and verification support, external memory blocking and configuration change history.

Bring Your Own Device is seen to be complex, expensive, and dangerous especially for Data Security

If employees are using their own devices, legitimate questions include:

- How can IT *protect the corporate data* from corruption, misuse, or theft?
- How can efficient use of company-owned applications be supported on *a device with non-standard configuration*?
- How can the employee install a needed application even when their device uses a *different operating system or operating system version*?
- Who *is responsible for taking care of his or her asset;*
- How can the organization protect centrally located data if it *can't ensure that a device is properly secured*?