PCM THE RIGHT TECHNOLOGY, DELIVERED™

Mobile Device Management for Your Enterprise

After attending our Secure Mobility Assessment, your organization will be ready to integrate smartphones, tablet computers, and any other mobile devices into your business workflow.

Secure Mobility Assessment

The number of organizations deploying mobile devices is increasing exponentially. We can show you how to manage these deployments (whether company-owned, bring-your-own-device, or a combination) to enhance productivity, decrease IT involvement, and maintain the security of your corporate data.

A Business Support Specialist is here to assist you.
Call today to learn more.

800-700-1000
www.PCM.com

With the proliferation of both corporate owned and bring your own devices (BYOD) interacting with corporate data, IT managers continue to struggle with the complex and ever expanding security risks. The 2014 Strategic Security Survey in Information Week noted that "managing the complexity of security" was the number one challenge experienced by IT managers. A key risk indicator identified by 58% of respondents was infected personal devices connecting to the corporate network, making it the No. 1 response, ahead of phishing and lost devices.[1]

Although initial IT costs go down with policies such as Bring-Your-Own-Device, these gains come with additional pressures on IT departments. Fortunately, IT has recourse: these Mobile Device Management systems can manage and mitigate these challenges via secure provisioning and device accountability.

Local Control for Distant Devices

Managing mobile technology at the enterprise level helps ensure both the security of the network and the protection of corporate data. Deployed mobile devices can be activated on-the-fly via SMS, e-mail, or using a Web- based interface. These options allow devices to be enrolled into a solution using authenticated user credentials, which configures settings and access to enterprise accounts.

Once enrolled, these devices can be provisioned for various levels of security, including mandatory passcodes, remote lock-down, audit trail generation, and quickly identifying non-compliant devices via monitoring. With configured alerts, IT can be notified of issues immediately and through periodically generated reports. With the ability to manage devices individually or in groups, IT can make granular or broad updates, changes, and settings adjustments over the air — all without any user interaction.

Satisfied IT Departments

The consumerization of technology has complicated the duties of IT, who must meet the new and varied demands of the users while maintaining security standards. Enrollment in a Mobile Device Management Solution allows users easy access to assets that they need to perform their duties and streamlines the enforcement of corporate mobile device policy.

Satisfied End-Users

Beyond security and stability, one of the key factors to Mobile Device Management is the superior user experience. With many of the elements of the infrastructure and access tied into the profiles, users no longer need to manage this information. With profile-configured VPN and network access, users do not have to hunt for corporate access and Wi-Fi keys. E-mail, contacts, and calendars configured by profile ensure that every user has access to their resources immediately. With Web Clips, uses have access to corporate sites, from HR to Operations and even Application catalogs.

Continued on back...

[1] *Source: InformationWeek 2014 Strategic Security Survey*

Secure Mobility Assessment:
A week of planning, a future of success

Achieving Success

Thanks to our long-standing relationships with Apple® and major MDM vendors, we can provide a full start-to-finish solution to help you be prepared for deploying mobile devices in your organization. Our intensive assessment is custom tailored to the needs of the customer. It starts with a detailed analysis of your existing infrastructure and then guides you through the entire process of reviewing the environmental factors that influence a successful deployment, understanding the possibilities of Mobile Device Management, and determining the key requirements for a successful large-scale rollout of managed mobile devices in your particular business environment.

Phase 1
Analysis

- Enterprise Mobility Overview
- Environmental Analysis

Phase 2
Education

- Mobility and Corporate Security
- Capabilities
- Limitations
- Risk Remediation

Phase 3
Policy

- Principles of Device Management
- Policies
- Business Case Development
- Use Case Development

Phase 4
Corporate Governance

- Mobility Practices
- Policy Paradigms
- Governance Review
- Workshop

Phase 5
Recommendations

- Requirement of Mobility
- Analysis Review
- Environmental Recommendations
- Mobility Recommendations