BoxTone®
Mobile Service Management

A CISO's Handbook

Enterprise iPhone & iPad Security & Compliance

Protecting Corporate Information as Your Workforce Goes Mobile

Why You Need to Read This Handbook Now

As mobile devices like the iPhone and iPad drive the consumerization of IT, the days of enterprises maintaining a single device platform are quickly fading. Fueling the change? These and other devices are more like "app phones," using laptop-like computing power to drive the maximum mobile worker productivity that management loves. This CISO Handbook explains how to extend an enterprise-grade security framework to devices running on the iOS 4 platform, including what's needed to securely and safely connect corporate-owned and employee-owned devices to new and existing enterprise applications and data.

The Workforce Goes Mobile and Security Threats Follow

As workers leave their corporate desks behind and spend more time in the field, the complexity faced by enterprise IT Security is exploding. Forrester Research found that at 32% of companies surveyed, one-fourth of the employees work in the field more than half of the day. And remote working is accelerating, as mobile devices, mobile applications and ubiquitous wireless access facilitate the use of information and services at the point of business.

The challenge for CISOs and their teams has been to adapt security best practices to this rapidly changing environment and ensure continued compliance with corporate policies. Starting in 1999, as shown in Figure 1, this meant that the brick-and-mortar focus of IT Security – which was centered on keeping Internet threats out – had to morph to accommodate mobile users, who first worked remotely on laptops but who later turned to BlackBerry, and now iPhone and Android devices.

Figure 1: Evolution of Enterprise Computing & Endpoint Security

Data, reputational and legal losses from misappropriated or misused devices that operate beyond the corporate firewall are serious business. In an infamous WiFi attack against a leading discount retailer in 2007, hackers gained access through a wireless regional hub for the company's store controllers that handled its point-of-sale system, grabbing sensitive information about more than 45 million customers. That breach resulted in the retailer paying $9.75 million to 41 states.

In response to similar threats, IT suppliers extended the security and compliance continuum to include data protection software on the laptop, coupled with secure WiFi and VPN access back to the datacenter. The desire for anytime access fueled the emergence of the BlackBerry smartphone for mobile email, embraced by IT for its seamlessly integrated advanced mobile device management which delivered comprehensive control via 420+ IT policies, over the air (OTA) application push and security control, and enterprise application white-list/black-list control.

From Smartphone to "App Phone"

But the latest iPhone, Android and BlackBerry devices have redefined what it means to be a smartphone, offering a variety of applications and modes of communication. Indeed, New York Times technology writer David Pogue has called the smartphone label too limited, preferring "app phone" to reflect the power of these devices beyond email.

Support from mobility platforms like Exchange ActiveSync and Lotus Notes Traveler have made it easier for employees to use their devices at work, leading to what industry analysts call the "consumerization" of enterprise mobility. The result? By 2013, the average organization will likely see 70-80% of its mobile users network-connected, with IT forced to support a dozen or more device types, three or more connectivity platforms and five or more enterprise mobile applications. And at least 50% of those devices will likely be employee-owned.

Unfortunately, if even one of these powerful devices – loaded with sensitive corporate information and access – is stolen, hit by a malware attack or simply left behind in a cab or restaurant, the potential for significant losses is real, perhaps as much as $121,000 to $1.5M per incident according to an Aberdeen survey. The same survey noted it was possible for one device to invoke multiple lapses of Sarbanes-Oxley (SOX, JSOX), Health Insurance Portability and Accountability (HIPAA), COBIT Operational Standards and other regulations.

This CISO Handbook focuses on how IT Security can extend the established security and compliance continuum to the iPhone and iPad by leveraging 3rd party MDM and Security Management software, coupled with the iOS 4 platform from Apple, to lead the way to improved mobile worker productivity and enhanced company value.

Holistic and secure mobile management can be described in five Parts (Figure 2).

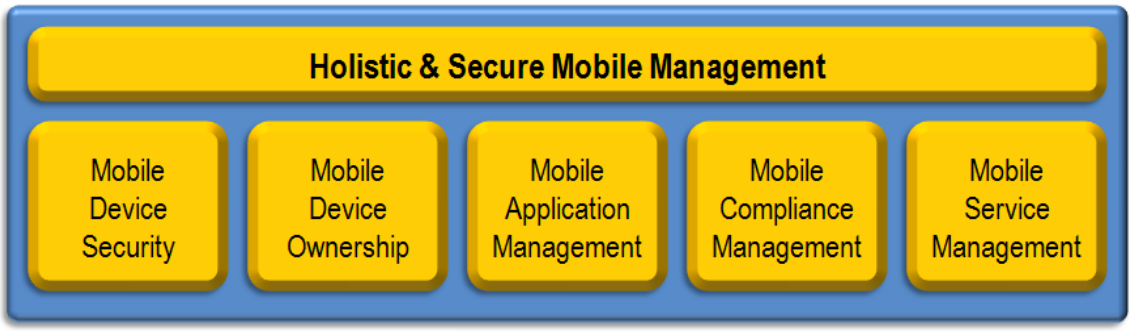

Figure 2: Five Parts to Holistic Mobile Management

Part 1: Mobile Device Security

While the latest mobile devices were built for consumers, device vendors have recently been enhancing them for the needs of the enterprise. For the iPhone and iPad, security and manageability on par with that for other mobile assets has arrived, in the form of iOS 4 coupled with 3rd-party Mobile Device Management and Security Management software from providers like BoxTone.

Data Protection

How to best secure the iPhone, iPad and other smartphones has a precedent. The first time a worker carried a laptop outside the physical confines of the office, that worker had become mobilized and a new security risk was born. Mitigating this threat required the use of password policy to control access to the device and data-at-rest (DAR) encryption to protect device contents.

IT Security can now extend proven laptop security policies to the iPhone and iPad. iOS 4 devices natively support device lock, hardware-based DAR encryption and remote wipe. The OS also continues to evolve its device security capabilities and recently added full "data at rest" and "data in motion" encryption of users' email, contact lists and specified application data. Enabled by 3rd-party MDM software, all of these capabilities can be remotely provisioned, managed and verified over the air, enabling IT to provide a secure end-to-end environment for key corporate applications, messaging and contact lists.

Resource controls

Using native configuration profiles and 3rd party MDM software, enterprise IT can mass-configure iPhones, iPads and other iOS 4 devices over-the-air in a consistent and verifiable way, preventing security holes that can be exploited by hackers. In addition, as shown in Figure 3, restrictions on device features like cameras, screen captures and web browsing can be explicitly enabled or disabled by policy.

Policy-Based Security

Native policy facilities vary by mobile operating system. iOS 4 provides a management framework that helps IT integrate the iPhone and iPad with existing datacenter infrastructure – such as email, VPN, WiFi and PKI – and security policies. Core to this approach is the configuration profile, a rich and robust construct that simplifies the administration of security policies and helps govern device capabilities.

Configuration files are XML-based and can be remotely applied and managed over the air with MDM software integrated with Active Directory or other LDAP solutions to simplify mobile security with group-based administration and application of policies.

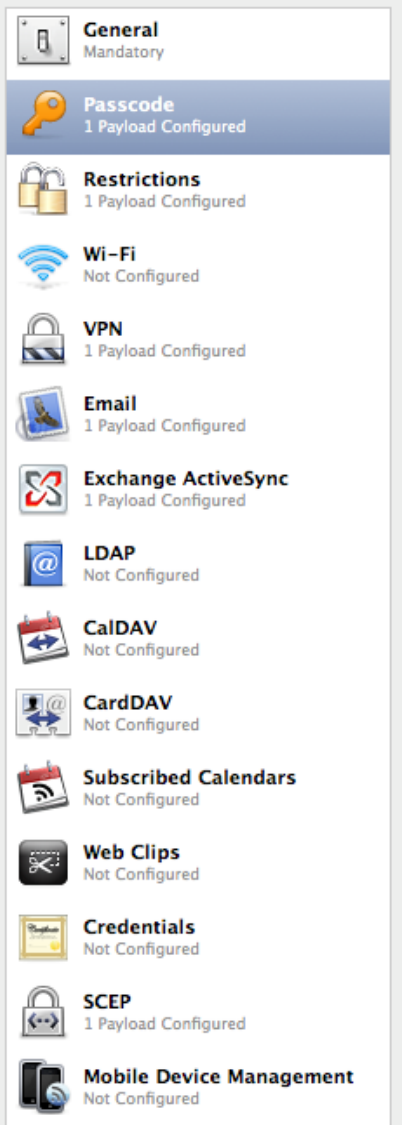

Figure 3: iPhone Configuration

Part 2: Mobile Device Ownership

A recent Aberdeen Group survey found that employee-owned devices now constitute 42% of all network-connected devices, representing a four-fold increase in just one year. At the same time, only 40% of companies now provide devices to their employees, a significant decrease from the previous year when 75% of companies supplied devices.

IT Security teams must quickly determine how to securely network-connect all of these personal devices without burdening IT resources, and while maintaining compliance.

Governing Employee-Owned Devices

Connectivity should be given only to those employees who sign-off on a corporate mobile use policy. The preferred approach is to include an electronic version of the agreement as part of the self provisioning and activation process.

Corporate information should also be segregated from personal information on iOS 4 devices, such as with a "secure virtual sandbox" offered by BoxTone, to simplify the management of corporate data throughout the device lifecycle. IT should use MDM software to selectively wipe clean corporate data when a worker abruptly exits the company or installs rogue applications. In other scenarios, such as a lost device, both the employee and the enterprise will want to fully wipe the device's contents.

Integration with the Datacenter

Using native configuration profiles and centralized smartphone management via MDM software, IT Security can leverage existing datacenter services – such as Active Directory (AD) and PKI – to establish and maintain a secure mobile environment. Group membership within AD ensures that users are not only authenticated, but also authorized to use their personal devices for work. In addition, AD integration allows IT to tailor device security settings to match the security posture of users and scalably apply policies via AD groups.

Part 3: Mobile Application Management

Business management loves mobile devices like the iPhone and iPad for two key reasons: they enable productivity improvement with applications beyond email; and they help employees better serve customers and business partners.

Security teams can support these initiatives by providing an open and protected framework for deploying new apps while protecting corporate data against malicious apps that employees might inadvertently bring to the workplace.

Secure and Standardized Framework

An optimal app deployment approach should be open and flexible, supporting multiple application frameworks that include web-based applications as well as thick apps written for the native OS SDK. Leveraging iOS 4 and 3rd-party MDM software, IT can control which apps are available to employees, making sure users are authorized before configuring secure access. IT can also use over-the-air device management to programmatically configure each device to fit the user's corporate role, set up secure network access (VPN, WiFi) to apps and provision the device with approved apps from an internal enterprise app catalog.

Figure 4: Common Software for iPhone Jailbreaking

Safeguarding Against Malware

Jailbroken iOS 4 devices – the process that allows iPad, iPhone and iPod Touch users to run third-party unsigned code on their devices by unlocking the operating system and allowing the user root access – can enable hackers to steal personal information, damage the device, attack the wireless network or introduce malware and viruses. Offers to jailbreak these devices are everywhere (Figure 4). And a jailbroken device is still able to use the App Store and iTunes. IT Security should take advantage of 3rd-party MDM software to identify hacked devices, and either prevent them from entering the corporate network or quickly quarantine them should they attempt to connect.

Part 4: Mobile Compliance Management

Smartphones can be more easily manipulated by technically savvy users who want to skirt around IT policies. So IT Security must continuously monitor and visualize mobile device compliance, mitigate issues and provide evidence of compliance to corporate auditors.

Active Enforcement

Compliance enforcement ensures the persistence of software, configuration and security policies on a device. IT Security should employ MDM and Security Management software to visualize device-level information including hardware version, software version, configuration profiles and security policies, as well as the authorization of each user and device. This software should actively enforce security controls at all times, identifying non-compliant devices and then automatically quarantining or cutting them from enterprise access, while making sure all enterprise data is locked until IT remediates the compliance issues.

Audit Reporting

IT Security should also be able to generate compliance reports to satisfy legal, corporate and regulatory auditing requirements. All device activity should be fully logged, and include users who are activated, deactivated or wiped; what applications are installed; and what corporate resources have been accessed. This information helps the organization identify newly attached

rogue or un-approved devices, while also verifying that upon any one employee leaving the company, a selective wipe was completed to clean corporate information from the device.

Part 5: Mobile Service Management

Securing the mobile environment is just one challenge of mobilizing a workforce and must be part of a larger framework to simplify and scale the use of smartphone technology within an organization. Best-in-class organizations are extending IT Service Management (ITSM) to highly distributed mobile environments via an approach known as Mobile Service Management (MSM).

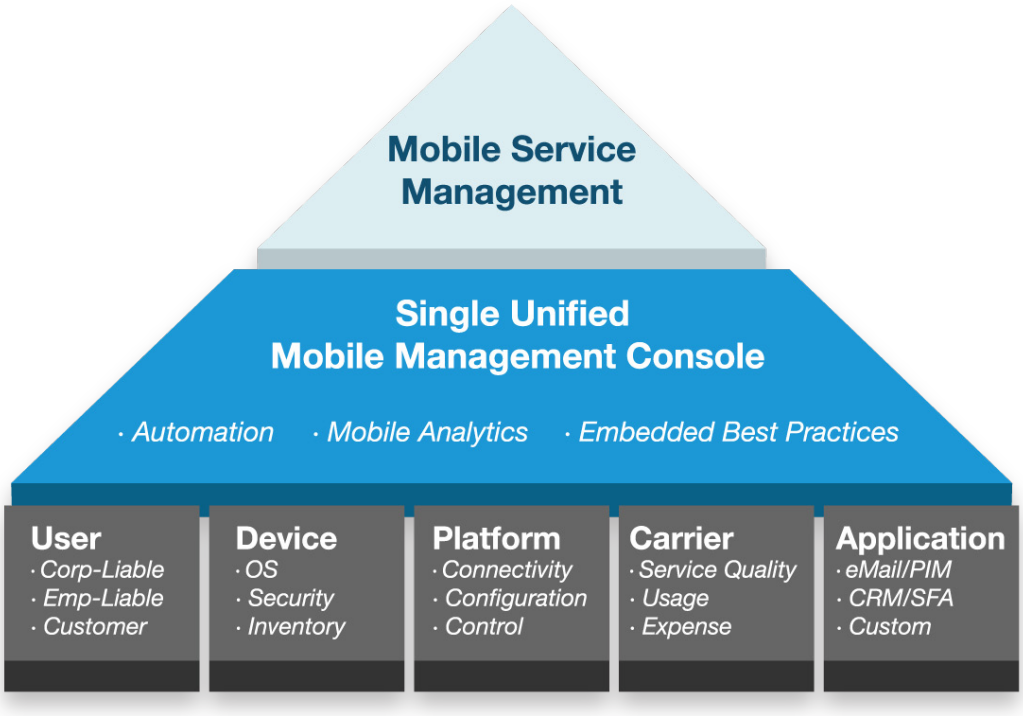

Figure 5: Proactive Mobile Service Management for the Enterprise

Mobile Service Management is a proactive, customer-focused approach for continuously delivering mobile IT services at the high quality that mobile users require, balanced with the reasonable cost and risk that IT and the business are willing to accept. Automated MSM software enables enterprises, government agencies and Managed Service Providers (MSPs) to centrally manage, secure and support all mobile devices, applications and platforms from a single, unified console.

More information on MSM can be found in: "Proactive Mobile Service Management: A Best Practices Guide for Threading Mobility Services into Core IT Processes," courtesy of BoxTone.

Conclusion

The demands from employees to network-connect mobile devices – like iPhones and iPads – are too loud to ignore and the benefits too substantial to disregard, despite the potential security challenges. However, it is essential to protect corporate information as a workforce goes mobile. Using a best-practices Mobile Service Management solution (which includes MDM and Security Management) that leverages the latest capabilities in iOS 4 for employee-owned and corporate-owned iPhones and iPads is within reach, with the CISO and IT Security leading the way to improved productivity of mobile employees and greatly enhanced company value.

BoxTone®
Mobile Service Management

About BoxTone

BoxTone's proactive Mobile Service Management (MSM) solution is trusted by more than 275 of the world's leading enterprises and government agencies, including 89 in the Global 2000, to continuously maintain optimal mobile performance & security at the lowest cost and risk. BoxTone's single unified mobile management console powered by patented automation technology addresses the entire mobile lifecycle: mobile device management, support management, operations management and business management. BoxTone delivers centralized control of all mobile devices including Apple iPhone and iPad, BlackBerry, Google Android, Nokia Symbian and Windows Mobile devices; mobile connectivity platforms including BlackBerry Enterprise Server, Microsoft ActiveSync and Good Technology; and enterprise mobile applications. Learn more from the expert in proactive Mobile Service Management (MSM) software solutions at www.boxtone.com, or call +1 410.910.3344.