

Towards Secure Mobility

Securely integrating mobile devices
into the enterprise



Executive summary

Today, knowledge workers comprise a significant percentage of the world's workforce, and the number continues to grow. As a knowledge worker, it becomes extremely difficult, if not impossible, to be effective without a personal computer or a phone.

At the same time, the way that knowledge workers interact with communications technologies continues to evolve. The advent of the mobile phone arguably changed business forever, and similarly, mobile computers such as laptops and notebooks have generated productivity and efficiency gains.

With Moore's Law in play, notebooks become smaller and mobile phones become more powerful, embracing ever-greater processing and computing power. The marriage of these technologies seemed inevitable, despite the complexity, failings and lacklustre adoption of early mobile computing devices.

One need only consider the widespread reach and dominance of Research In Motion (RIM)'s BlackBerry solutions into both enterprise and consumer markets today¹. The BlackBerry arguably redefined the market and set the standards against which other key players such as Apple, with iOS, Microsoft with Windows Mobile, Google with Android and various vendors using the Symbian Operating System, are judged.

The industry has reached a watershed moment. Mobile devices have become inexpensive enough to be affordable for non-corporate users, driving explosive adoption.

Accelerating this trend is the resurgence of tablet computing, primarily driven by Apple's iPad. The iPad has taken traditional tablet computing and brought it to the mainstream by creating visually appealing, purpose-built devices with simplified interfaces, and pricing these very competitively.

The value of such tools in business cannot be overstated, and as a result, employees – from executives to the technically savvy – who own such personal devices put pressure on corporate IT teams to facilitate the use of these tools in the corporate setting. Against this growing pressure, many organisations enable and encourage the use of these tools to facilitate productivity and attract the modern workforce.

This trend has spurred the demise of the traditional corporate perimeter, with a sudden flood of devices that are no longer directly managed and controlled by the enterprise accessing corporate resources. With the business drivers loud and clear, technology and security professionals are no longer able to credibly represent a roadblock for the adoption of mobile technologies.

While the loss of control over end-user computing devices is in itself a major risk and concern, the ability for the endpoint device to be very easily lost or stolen is a major additional consideration. Questions around the support and management of these devices and the risk and security implications of allowing them into the corporate environment continue against the backdrop of growing adoption.

A myriad of risks and threats are introduced to corporate environments as a result of the use of mobile devices. Serious considerations exist around the security of information and data, as well as compliance, when mobility is brought into the mix.

Conversely however, mobile devices do inherently provide significant security

benefits when compared to traditional personal computers. In many cases, a default configuration of such a device out-of-the-box is robust in many ways due to the design of the device. Additional measures can be taken to further harden these devices and lessen the risk posed to an acceptable level.

This paper will delve a little deeper and outline some of the factors driving increased adoption of mobile devices, the risks posed by these devices and some mitigating factors that the devices themselves incorporate.

The discussion will generically cover BlackBerry, iOS devices (iPhones and iPads), Android devices, Windows Mobile devices and Symbian devices without focusing on any single platform. Each of these has unique features, benefits and drawbacks, however an overarching approach will be followed, and will deal with these devices as a larger category of mobile devices.

Next, we'll outline some security considerations for organisations that wish to integrate mobile devices, spanning governance, risk and compliance, security policy, technical security controls and finally assessment and testing to highlight and validate potential shortcomings or vulnerabilities.

This journey towards a mobile workforce need not necessarily be fraught with risk and uncertainty. With some focus – and a change in mind set – secure mobility is achievable and will enable organisations to unlock the benefits that this new paradigm and underlying technologies promise.



¹ <http://communities.bmc.com/communities/blogs/unwiringit/2010/04/19/smartphone-market-share-data-blackberry-still-dominant-iphone-and-android-catching-up>

Key drivers for adoption of mobile platforms

A number of trends and developments are driving increasing adoption of mobile devices and the rollout of mobility solutions for employees.

The subsections to follow will briefly outline some of the key trends.

Increasing enterprise adoption

Today, many organisations recognise the value of enabling key employees with the tools and resources to work without needing to be physically at their desks.

Mobile phones, laptop computers, wireless networks and Virtual Private Networking (VPN) were early tools in enabling mobile workers. The market further evolved to incorporate video conferencing, and finally RIM introduced the BlackBerry, which further revolutionised business communications.

The smartphone market grew rapidly, and today devices ranging from iPads to Android smartphones are common within organisations. Technologies such as unified and converged communications enable seamless switching between mobile networks and wireless corporate networks, to enable employees to be reachable on a single number, regardless of their physical location or the device they are using.

Today, it is possible – and increasingly becoming expected – to use a device that fits readily into your pocket to communicate via traditional voice, Voice over IP (VoIP), e-mail or instant messaging. You can browse the web and access digital music, video and books or magazines. This has driven many organisations to begin offering support for these devices.

Today, it is possible – and **increasingly becoming expected** – to use **a device that fits readily into your pocket** to communicate via traditional voice, Voice over IP (VoIP), e-mail or instant messaging

Consider the numbers presented in a recent Forrester report³:

- 70% of North American and European companies support BlackBerry devices today
- 41% support Windows Mobile devices
- 29% support Apple iOS-based devices
- 13% support Android-powered devices

According to a recent Gartner report⁴, CEOs and CTOs should not ignore the iPad, as this will be a top strategic technology for 2011.

Bloomberg BusinessWeek recently published an article⁵ that highlighted major Fortune 500 corporations' focus on testing of Apple's iPhone, as a potential alternative or replacement for BlackBerry devices. Many organisations are similarly field-testing Google Android-based devices.

Dimension Data's own clients have shown increased interest in understanding the security implications of mobile devices such as iPads, and how to integrate these devices into governance, risk and compliance frameworks.

Growing impact of employee-owned devices

The adoption of personal computing devices that are not PCs is on the rise. Some analyst estimations indicate that new sales of non-PC computing devices will overtake PC devices by the end of 2010⁶.

Morgan Stanley's Internet analyst, Mary Meeker, predicts that in the next five years, more users will connect to the internet over mobile devices than traditional PCs⁷. Meeker says that adoption of Apple devices such as the iPhone and iPod Touch for the purpose of internet access is taking place more than 11 times faster than that of AOL and several times faster than that of Netscape in the early 1990's.

Employees who own such devices also want to use them in performing their jobs. As a result, corporate technology departments are under pressure to enable employees to use personally owned devices to access various corporate systems and resources. Forrester states that 56% of enterprises allow personally owned smartphones to access company resources⁸. This number is expected to increase.

...corporate technology departments are **under pressure** to enable employees to use **personally owned devices** to access various corporate systems and resources

3 Security in the Post-PC Era: Controlled Chaos – Forrester

4 Top 10 Strategic Technologies for 2011 - Gartner

5 <http://www.businessweek.com/news/2010-11-05/bank-of-america-citigroup-said-to-test-apple-s-iphone.html>

6 Forrester Research eReader Forecast, 2010 to 2015 – Forrester

7 Mary Meeker, Morgan Stanley – Internet Trends, April 2010

8 Security in the Post-PC Era: Controlled Chaos – Forrester

Mobility and unified communications

Mobility of employees has been a significant trend in recent years, with growing numbers of employees in many corporations working remotely.

Technology has supported this transition, through developments in VPN technologies, Instant Messaging (IM) and converged communications including VoIP and videoconferencing solutions.

Cisco recently published the Cisco Connected World Report⁹ which included a number of insights on mobility based on the responses to a survey conducted by Cisco of over 1300 key IT decision makers and end users, across 13 countries.

Key conclusions drawn in this report include the following:

- 60% of employees believe that they don't need to be in the office to be efficient
- 66% of employees desire mobile work flexibility
- 66% of employees would accept a lower-paying job with more mobile work flexibility than a higher-paying job with inflexibility
- Real-life consumer trends and an increasing number of devices in the workplace are causing employees to question the relevance of IT policies and break them
- IT policies need to keep up with a workforce that is demanding to be connected anytime, anywhere, with any device and access any information, or employees will do so, regardless of IT policy
- The use of video is on the rise for consumer and enterprise communications – almost seven in ten IT professionals expect the use of video to increase



The convergence of voice, video and data onto a single network platform has largely driven advances in technologies such as converged communications, allowing an employee to move between physical locations and networks, and still be reached at a single number.

Effectively, this allows an employee to use a smart device to send and receive voice calls, e-mail, conduct and attend video calls and videoconferencing, as well as access key business applications. This is all possible regardless of whether the underlying network medium is the corporate LAN, the user's home network, a public wireless network, or the wireless service provider's mobile data network.

For highly mobile users, smaller devices and longer battery life become essential. This significantly increases the appeal of smartphones and devices such as the iPad.

Consumer-focused mobility-specific platforms

One of the key drivers of device adoption is the purpose-built platforms to support them. These provide an intuitive and functional user interface that enables individuals to interact easily with the device.

Mobile devices have evolved both aesthetically and functionally, with a range of options to choose from, ranging from full QWERTY keyboards to touchscreen and voice-controlled interfaces. Many can easily be slipped into one's pocket or held like a small book or magazine.

The operating systems of these devices are built to enable messaging and communications with a simple user interface. An example of the wisdom of this approach to operating system design is Apple's alignment of its upcoming release of the OS X Lion operating system – modelled very closely on the iOS deployed across Apple mobile devices¹⁰.

Another key development in this area is the manner in which these platforms integrate applications.

Traditional applications designed for personal computers are complex, and hook into various areas of the operating system and file system, deploying numerous separate files. The deployment and management of these applications has traditionally been the responsibility of the technology department.

The concept of mobile applications has changed that model significantly. Applications are self-contained which limits them to their own environment on the mobile device. This has certain security benefits, which will be expanded on later. Many applications are selected and added by the users themselves as opposed to being installed and managed by corporate IT.

Clearly, reduced-function mobility-specific platforms, combined with applications that the user selects to enhance productivity, present a new and efficient way of working for many employees.

9 http://newsroom.cisco.com/dlls/2010/ts_101910.html

10 <http://www.apple.com/macosex/lion/>

De-coupling of services and endpoints

The adoption of cloud computing and Software-as-a-Service (SaaS) continues to accelerate. Cloud-based vendors' offerings range from consumer-focused file-sharing solutions, such as Dropbox¹¹, to enterprise solutions for employer services, such as payroll, benefits and HR, and IT service management (ADP¹² and Service-Now¹³, respectively). This only represents a fraction of the available services.

Many organisations are also considering this service model for internal delivery of applications and core functions as a service, through private cloud or hybrid cloud solutions, either on-premise or off-premise.

With cloud computing, accessing services requires very little core processing power, and not much more than a browser and an internet connection. This aligns well with mobile devices. If core applications are delivered via the web, then any device with web capability is able to access these services and applications.

Trends within the application marketplace for many devices validate this development, with mobile applications for services ranging from Salesforce.com, through Cisco's WebEx conferencing software¹⁴, down to interfaces to online trading solutions, such as E-Trade financial¹⁵.

As more and more software and applications are delivered as a service via the web, the barriers to working fully from mobile devices will be removed, driving more widespread adoption of these devices.

Inherent mobility-related risks

While the benefits that mobile devices can bring to the corporate environment are compelling, mobile devices by their very nature introduce various risks to organisations.

Organisations need to gain a clear understanding of the security implications and how to integrate these solutions without exposing themselves to unacceptable risk.

This section briefly outlines some key areas of risk that mobile devices introduce, some of the mitigations of these risks that are built into the platforms and devices themselves, and finally additional steps that enterprises can take to further reduce risks.

As a first step, however, it is important to explore the risks themselves.

Organisations need to gain a clear understanding of the security implications and how to integrate these solutions without exposing themselves to unacceptable risk.

Support and management of devices

Traditional endpoints in corporates are procured, configured, and deployed by the technology department. These endpoints are often the products of a single vendor, with a base desktop build that is fully configured and managed to be consistent across the environment. This makes them easy to manage and support with enterprise tools.

The same does not hold true for mobile devices. While in many organisations today, BlackBerry is the device of

choice, and some standardised form of management via the BlackBerry Enterprise Server (BES) exists, this is changing as users bring in other kinds of devices. Standardisation and management of device hardware and software is not possible in such an environment.

Organisations need to evaluate the software and service offerings that are available to addressing this issue. Vendors provide some basic tools and a market for management software for mobile devices does exist, however the market is still immature, relatively unfamiliar to most organisations, and has seen considerable consolidation and recent activity¹⁶.

In many cases, the technology will still need to be proven, and enterprises will look to extend technology that they have already deployed for management of endpoints to also cover mobile devices. Vendors may not be at that point yet, which stalls adoption within organisations or forces them to add additional vendors into their product stable.

This paper will not examine the implications of the adoption of IPv6, however it does bear mention. As the number of devices that require network access grows, organisations will find that traditional IPv4 solutions can no longer handle the addressing requirements of increasing numbers of mobile employees.

As a result, organisations will need to prepare for an IPv6 rollout. Initially, this may require two separate networks, to support both IPv4 and IPv6, until such time as a full migration to IPv6 has been completed.

Organisations also need to consider the blurring line between what belongs to them and what belongs to the employee. A user-owned device is undoubtedly used for personal communication as well as to access corporate resources and applications. This makes the relationship between the employee and corporate IT more complex and raises the question as to what demands corporate IT can make on device configuration of employee-owned devices.

The blurring of personal and corporate resources introduces many questions for organisations around the protection of their data. Currently, there is lack of clarity from a legal perspective regarding data ownership, data protection responsibilities and privacy guidelines, with case law still far from definitive.

Organisations need to gain a **clear understanding** of the security implications and how to **integrate** these solutions without exposing themselves to **unacceptable risk**

11 <http://www.dropbox.com/>

12 <http://www.adp.com/>

13 <http://www.service-now.com/>

14 <http://www.webex.com/apple/>

15 https://us.etrade.com/e/t/mobile_pro/iphone

16 For example McAfee's acquisition of Trust Digital

Ownership of data

An additional grey area linked to the previous point is the ownership of data stored on the mobile device.

The blurring of personal and corporate resources introduces many questions for organisations around the protection of their data. Currently, there is lack of clarity from a legal perspective regarding data ownership, data protection responsibilities and privacy guidelines, with case law¹⁷ still far from definitive.

The matter is even more challenging for organisations that handle regulated data and need to ensure that it is adequately protected.

For example, in the healthcare industry, employees, nurses and doctors can attend to patients and update patient records using a mobile device such as iPad. The Health Insurance Portability and Accountability Act of 1996 (HIPAA) Security Rule¹⁸ has mandated organisations to implement appropriate safeguards, information security policies, procedures and controls to protect electronic Protected Healthcare Information (ePHI).

In addition, the Health Information Technology for Economic and Clinical Health Act (HITECH)¹⁹, has added to the pressure on healthcare organisations and their business partners with respect to the management and protection of electronic healthcare information.

The same applies to organisations to which the Payment Card Industry Data Security Standard (PCI DSS)²⁰ is applicable, as well as other organisations dealing with sensitive data, or other forms of Personally Identifiable Information (PII).

This poses a number of questions for risk and compliance officers and security professionals around the portability of such data via mobile devices, and what steps can be taken to protect the data.

Theft and loss

The small size and portability of mobile devices coupled with their mass appeal means they are very easily lost, left behind in cabs, planes and trains, and present attractive targets for theft.

Consider the following statistics:

- Business travellers lose 12,000 laptops per week in North American airports
- 63% of small to medium business have lost devices within the last year
- 58% surveyed have lost data within the last year
- 100% of organisations surveyed have devices that do not support remote wiping of data
- 42% of data breaches in North America occur due to lost or stolen data-carrying devices

One incident that received a lot of press coverage was the loss of a prototype of the Apple iPhone 4 prior to its release²¹. An Apple engineer who was field-testing the new device was said to have left the device in a bar in Silicon Valley. Technology blog site Gizmodo paid the patron who found the device \$5,000 and acquired this device, releasing pictures and a full report of the upcoming technology.

The implications of the loss of a device can be even more catastrophic when one considers the regulations in place around data protection. This remains a key concern for organisations deploying mobile devices.

The blurring of personal and corporate resources introduces many questions for organisations around the protection of their data. Currently, there is **lack of clarity** from a legal perspective regarding **data ownership, data protection responsibilities and privacy guidelines**, with case law still far from definitive

18 <http://www.hhs.gov/ocr/privacy/hipaa/understanding/index.html>

19 <http://www.hipaasurvivalguide.com/hitech-act-text.php>

20 https://www.pcisecuritystandards.org/security_standards/documents.php?document=pci_dss_v2-0#pci_dss_v2-0

21 http://www.cbsnews.com/8301-501465_162-20003447-501465.html

User control over application deployment

A key difference between traditional endpoint devices and mobile devices is that with mobile devices, the technology department no longer controls deployment and configuration of applications – this choice is made by the user of the mobile device.

Mobile application repositories such as Apple's AppStore, the Android Market and BlackBerry App World allow users to discover new applications and install them at the click of a button. This can be done independently of the corporate technology department, and without its approval.

Further complications arise due to the fact that a large proportion of applications available to users have been developed by other users. While vendors can provide some measures of visibility and screening, it is not uncommon for applications to perform functions without the user's knowledge, such as transmitting data about the user and device to external web servers²².

The impact of such malicious applications ranges from tracking a phone's location, stealing contacts, viewing text messages and sending text messages to paid text services, racking up unauthorised fees. This poses a considerable threat when users are not in a position to understand the permissions that they approve for applications during the installation process. This threat is aggravated in cases where the platform is more open by nature (such as Google's Android) or where users circumvent some of the built-in security measures (in the case of jailbroken iPhones).

...the very nature of many of the mobile devices keeps them a **permanently connected** and network-enabled target for attackers

Jailbreaking an iPhone, for example, may hamper management efforts, expose the user to more threat from malicious applications, and in many cases exposes users to threats that they may not even be aware of. This was seen in the case of the iPhone worm of 2009 that exploited a flaw in jailbroken iPhones²³.

Naturally, this represents a marked shift for corporate technology and security departments that are accustomed to controlling the software that can be installed on endpoints, often after undertaking risk and technical assessments on such software before approving it for corporate use.

Accessibility and attractiveness

The very nature of a mobile device is that it is switched on and accessible for most, if not all of the time. Many people, particularly corporate users, never power their devices off.

This presents an attractive target for attackers. Users may not always have endpoint workstations such as desktops and notebooks powered up and connected to the network, but the very nature of many of the mobile devices keeps them a permanently connected and network-enabled target for attackers.

In addition, the prospect of a single target leading to an opportunity to compromise multiple communication channels is attractive to an attacker.

Today, many out of band communication and authentication mechanisms use voice or text messaging as a medium. For example, financial applications send One-Time Passwords (OTP) and Transaction Verification Numbers (TVN) to the users' pre-configured mobile numbers.

If an attacker were able to compromise an endpoint that comprised both the primary data channel and the secondary out of band communications channel, this would be a significant advantage.

Human weakness

The human element of security has always been the very weakest link in the chain. Despite numerous attempts at user education and awareness, the vast majority of compromises today may be traced back to a human weakness. Many of the attacks targeting users today are technically sophisticated to the point that even savvy users fall prey to them.

Issues such as SPAM and social engineering, malicious applications and similar attacks are now delivered via a new platform, where users may not be able to recognise some of the tell-tale signs of such behaviour that they have grown accustomed to when using personal computers.

Untested platforms

There has recently been renewed interest in mobile devices and mobile platforms. While some attackers have been attempting to penetrate mobile platforms for a number of years, newer platforms such as iOS and Android have only started to receive serious attention from the security research community (those with noble, as well as those with malicious intent) in the more recent past.

This means that for the most part, as an industry there is a lack of clarity as to how vulnerable these platforms actually are. On a daily basis new data is released on insecurity in mobile platforms, such as the report recently released by Coverity on the high number of vulnerabilities in the Android OS²⁴.

This is a stark contrast to traditional endpoint platforms that have been subject to attacks for years and have been extensively tested to provide a more informed understanding of their security posture.

As this technology space gains traction, security research will accelerate and as an industry, a greater understanding of the threats in these platforms will be achieved.

22 <http://blogs.forbes.com/andygreenberg/2010/11/10/when-angry-birds-attack-new-android-bug-lets-spoofed-apps-run-wild/>

23 <http://www.tuaw.com/2009/11/23/new-jailbroken-iphone-worm-is-malicious/>

24 <http://www.darkreading.com/insider-threat/167801100/security/vulnerabilities/228200043/hundreds-of-software-flaws-found-in-android.html>

Mobile device risk mitigating characteristics

The threats associated with mobile devices are considerable. However, the inherent differences between these devices and traditional computing platforms do provide a number of benefits that serve to mitigate some of the risks.

In fact, it is arguable that some of these devices have a stronger security posture than personal computing devices by default. This is due to a number of complementary platform design aspects and features, several of which will be outlined in the following sections.

Purpose-built platforms

The operating systems that power mobile devices are based loosely on traditional operating systems, in many cases derivatives of *nix²⁵ or Windows, however they have been stripped-down and designed with mobility and communication in mind.

The mobile platform design methodology means that a large number of unnecessary components are not included in the operating system, which results in a more streamlined operating platform. Complexity is the enemy of security, and in this case, the elimination of excess functionality results in a smaller exposed attack surface.

In addition, in many cases these devices have no actively listening network services to accept inbound connections. The platforms themselves also run less active processes, and are in many cases constrained as to the level of extensibility and plug-ins available to users. All of this reduces the attack surface.

In many cases an out-of-band communication channel is built into the device itself, in that the device supports text messaging outside of the IP communications channel. Devices that use SIM cards also provide smart-card capabilities via the SIM, with an additional unique identifier. This can be extremely beneficial in the case of multi-factor authentication.

Ultimately, the fact that attackers have less to aim at reduces the chances of devices being compromised.

Default hardened security posture

Mobile devices and operating systems have the benefit of being architected and developed in more recent times, where there is a more heightened awareness and sense of security.

Vendors have approached the design and architecture of such platforms with security in mind from the very beginning, and in many cases without the need to incorporate legacy code with its associated vulnerabilities. This results in many design decisions that greatly benefit the default security posture of the devices themselves.

Most devices today support hardware-based encryption of data, as well as software and application encryption for some earlier models. Vendors have also considered issues such as code-signing and sandboxing, which mitigate the risk posed by a single application, by limiting that application to its own allocated resources and preventing a single compromised application from compromising others.

For example, Apple's iOS device even incorporates trusted firmware that forms part of the chain of validation for developer code, and developer code must be controlled and approved by Apple before being checked into the AppStore.

By nature, mobile platforms are also more resistant to malware, which remains a persistent frustration for corporate technology and security departments. Much of the common malware that infects personal computers is thwarted by the combined security measures built into mobile platforms.

This does not mean that these devices are not prone to vulnerability. Attacks have targeted iOS systems, and most recently a flaw in the handling of Portable Document Format (PDF) files could be exploited if the user browsed a malicious page in Safari, leading to code execution on the platform²⁶. This flaw was used to enable the most recent iOS jailbreak.

A recent vulnerability in WebKit was exploited in a way that would grant an attacker a remote shell on the affected Android device if the user browsed a malicious site. The security researcher published the exploit code publicly in early November 2010²⁷.

In November 2010, a worm targeting the Symbian Operating System was reported to have infected over a million mobile phones in China²⁸. The worm continually sends text messages from infected devices, racking up charges for users. This malware further targeted the human element – the code was embedded within a fake anti-virus application.

Security researchers have also published papers detailing attacks on mobile platforms that received much media attention, indicating that these platforms are not immune to targeted attacks.^{29 30 31 32}

At initial glance, this may seem overly concerning. However, as highlighted in a recent Forrester report, the combination of vulnerabilities reported across the iOS, BlackBerry OS and Android mobile platforms since 2008 is less than one-fifth the number affecting Windows PCs³³.

Despite the presence of these and other vulnerabilities, effective exploitation of the flaws is made much more complex by the additional security measures built into the mobile platforms.

25 Unix, Linux

26 <http://www.vupen.com/english/advisories/2010/1992>

27 <http://www.exploit-db.com/exploits/15423/>

28 http://news.yahoo.com/s/digitaltrends/20101111/tc_digitaltrends/zombievirusinfects1millionchinesecellphones

29 <http://securityevaluators.com/content/case-studies/iphone/>

30 <http://www.slideshare.net/y3dips/attacking-blackberry-for-phun-and-profit>

31 <http://www.scmagazineus.com/new-attack-targeting-windows-mobile-phones/article/121014/>

32 http://mulliner.org/pocketpc/feed/CollinMulliner_syscan07_pocketpcmms.pdf

33 Security in the Post-PC Era: Controlled Chaos – Forrester

Vendors control security

One of the major benefits of mobile platforms is that the vendors themselves have greater insight into the security of the platform.

On the one hand, much of the need for after-market third-party security products that have become standard on personal computers has been eliminated. While anti-malware solutions do exist for mobile platforms, in many cases these are unnecessary for the majority of organisations. Steps previously outlined, such as code signing, play a significant role in embedding the vendor into the security process for applications.

In addition, the vendors have increased developer accountability in many cases, by becoming involved in the review and approval process for applications that are developed prior to these being published in the public application repositories for the relevant vendors and platforms.

This is by no means foolproof as is clear from the reports of malicious applications that have surfaced, targeting multiple platforms. However this does go a long way toward increasing developer accountability and keeping the vendor firmly in control of platform security.

Basic remote management capabilities

RIM has set a high standard for enterprise management of mobile devices with its BES solution.

The BES solution allows corporate technology and security teams to specify detailed policy and retain a high level of control over BlackBerry devices in the enterprise. This has helped keep RIM ahead of its competitors, as no other native solution currently exists to manage other devices to the level that BES offers to the enterprise.

Apple provides some out-of-the-box capabilities for over the air management of iOS devices, however the inherent support for Microsoft® Exchange ActiveSync in newer versions of iOS has opened the concept of iOS devices in business to most organisations. ActiveSync allows for more rigorous control over the air of iOS devices, as well as Android devices. While not on the level of BES, this is a very appealing development for many organisations.

In many cases, organisations are able to exert some form of influence, either via configuration template or over the air, to apply technical policies and lock down certain behaviour of mobile devices. This provides an initial step in integrating such devices into enterprise networks, and it is expected that this capability will evolve as the mobile platforms themselves advance.



Key considerations for enterprise adoption

Mobile devices and the platforms that power them do inherently introduce certain risks to organisations looking to adopt and integrate these solutions.

Some of the risks are mitigated by characteristics of the devices themselves, but there are some additional steps organisations should take if they are aiming to integrate mobile devices without introducing unacceptable risks.

The sections to follow will outline some key considerations and recommendations for organisations integrating mobile solutions, to address information security requirements across the entire lifecycle. These suggestions will cover governance, risk and compliance, policy and procedure, technical controls and implementation and testing and assessment.

This will ensure that organisations carefully consider and address key focus areas that will ultimately reduce the risk profile of mobile solutions.

Governance, risk and compliance

Governance, risk and compliance are the cornerstones of an effective information security management framework.

A critical aspect of secure mobility is a thorough understanding of information and data management within an organisation. It is essential to know what data is considered critical and what the organisational policy on protection and handling of that data is.

This is best achieved through a robust data classification system that is actively followed and strictly enforced. The sensitivity labels applied to various organisational data will dictate how that data should be handled, and can drive risk assessment, policy and controls around that data in alignment with the overall organisational guidelines.

It is also important to have a clear understanding of situations where data must be protected in order to comply with the regulations affecting the organisation. Without this insight, it is not possible to properly align policy and technical controls.

Mobility affects many aspects of a company's information security architecture. Success requires that organisations incorporate the security of data throughout all aspects of risk assessment and evaluation, as well as all compliance efforts.

Mobile communications policies

Once an organisation has a thorough understanding of the risk profile and the implications of the mobility solution on data security governance, it should review and refresh its policies and procedure to incorporate and cater for the mobile solution. Where relevant, new policies should be developed to specifically address mobile devices.

Key aspects of policy and procedure to be addressed include an overall policy for mobility management.

This policy should address the following aspects applicable to the mobility solution:

- A specific statement outlining whether company-provisioned or owned devices are permitted exclusively, or whether employee-owned devices will be permitted to access corporate resources
- The process for device management, whether it be over-the-air or configured with static templates by corporate IT, and the specific technologies in use
- Which devices will be fully supported, which will be partially supported and which will be unsupported
- Minimum standards for supported devices, in terms of the nature of management that the device supports, the security measures that can be implemented on the device, and the overall data protection profile of the device
- Whether any specific devices will be explicitly disallowed from accessing corporate networks and resources
- The impact on corporate wireless networks and wireless network configurations
- The security measures and configuration templates that will be applied to mobile devices per the data that they access and the nature of the device

- The policy pertaining to installation and management of installed applications, permitted applications and expressly disallowed applications
- Guidance around the process for internal development of mobile applications, and the security controls built into this Software Development Lifecycle (SDL)
- Any technical measures pertaining to management of application deployment, and the necessary evaluation procedures and approval steps before an application is considered acceptable for deployment
- Any high security or higher assurance configurations for devices specifically accessing regulated and protected data
- The approach to data handling, and an indication of whether endpoints will be treated as untrusted, and what data and applications they will be permitted to access and in which format, if treated as untrusted
- Linkages to and tie-ins with the appropriate Acceptable Use Policies
- An official standpoint on the privacy of data, and the organisation's right to monitor data and seize devices in the case of incidents and investigations
- Forced acceptance of the mobility security policy prior to connection of the device to corporate resources
- Incident reporting and response policies, specifically around theft or loss of mobile devices
- Secure disposal and cycling of devices, and data wiping policies

Acceptable Use Policies must also be updated to specifically address mobile devices and what is permitted and not permitted. This is a critical step that must be handled with care.

Overly restrictive policies **may alienate** users and result in the violation of such policies



Much of the appeal of mobile devices is the freedom that they offer users to interact and collaborate. Overly restrictive policies may alienate users and result in the violation of such policies. Careful planning and interaction with users will ensure that the policies allow users the level of freedom that they value, while balancing the risk to the organisation appropriately.

Technical security policy and controls

Once policy has been designed and outlined to align with the governance, risk and compliance drivers of the organisation, technical security policies and controls can be developed to enforce these policies and then be deployed to mobile devices.

Controls will be designed per the device and platform in use, and the capabilities of such devices when paired with the deployed management platform. Once more, in the case of devices dealing with sensitive and regulated data, more restrictive policies must be deployed.

The key in this phase is to deploy controls that balance the risk profile of the device, the role of the user, the data that will be accessed, and the minimum acceptable security posture of the organisation taking into account all of the other factors.

Control areas should cover the following facets at minimum:

- Control over application deployment and permitted applications
- Control over cameras and other imaging functions of devices, including screen capture
- Control over browsers
- Control over permitted media recording and playback
- Control of explicit or inappropriate content
- Authentication controls, including complex alphanumeric passwords, auto-locking of interfaces, and strong authentication such as certificate-based authentication
- Technical controls around caching of credentials on the device
- Encryption, whether at a hardware level, for specific applications, or via VPN
- Wiping of data after multiple failed unlock attempts, as well as remote wiping of data
- Control of Bluetooth and wireless functionality
- Continual refresh and re-application of applicable technical policy
- Protection and encryption of device backups
- Protection of configuration templates and security profiles

These technical controls will expand on the default security offered by deployed mobile devices and will help the organisation align the mobility solution with the acceptable risk profile outlined in the risk assessment conducted as the initial step of this programme.

Testing and assessments

Design, definition and architecture of policy and technical controls to align any solution with organisational risk expectations and compliance benchmarks are important steps. However, their value will be eroded without testing and assessment to validate the effectiveness of these solutions in mitigating risk.

Once technical controls have been implemented, organisations should conduct an assessment of the mobility solution and endpoints, in order to highlight and demonstrate any vulnerabilities and flaws that may have been overlooked.

A key aspect of this is to assess the security posture of in-house developed applications, especially if these applications will be deployed to clients. The source code of these applications should be reviewed, and where relevant, the applications should undergo some form of penetration testing.

For organisations adopting third party or external applications, where relevant, these applications should also be assessed to determine whether they incorporate any malicious functionality, backdoors or other unwanted characteristics.

Even in cases where the source code is unavailable, the applications can be subjected to static binary or dynamic analysis to attempt to determine whether they demonstrate any unwanted behaviour.

It is only through a consistent cycle of planning, design, development, implementation and testing and assessments that risk can truly be managed to an acceptable level.

Success requires consideration of the security implications of key aspects of the mobility solution, and careful planning to address information security in line with the fundamentals of a mature information security programme:

- Governance, Risk and Compliance (GRC)
- Policies and guidelines
- Technical security policy and controls
- Testing and assessment

It is also important to bear in mind that despite popular media hype around the flaws and vulnerabilities of mobile devices and platforms, many of the underlying causes of these flaws are not new.

If one considers trojaned or malicious application as an example, the security industry has been cautioning on the dangers of running untrusted code, or running code without understanding the full ramifications of its effect on a system, for many years. This is no different on mobile platforms.

Vulnerabilities affecting mobile browsers do pose a considerable threat – but an arguably greater threat is posed to traditional personal computers by these very same flaws. Endpoint security principles are important whether a device is pocket-sized, or located on a corporate desktop.

Conclusion

Mobility promises vastly increased productivity and effectiveness of employees, and is a very necessary step in the continued evolution of business. Forward-looking organisations realise that they do not really have a choice whether to 'go mobile' or not, it is already happening. Nevertheless, it can – and should – happen securely. The journey towards a mobile workforce need not necessarily be fraught with risk and uncertainty. With some focus, secure mobility is achievable and will enable organisations to unlock the benefits that this new paradigm and underlying technologies promise.

MIDDLE EAST & AFRICA

ALGERIA • ANGOLA
BOTSWANA • CONGO
DEMOCRATIC REPUBLIC OF THE CONGO
GABON • GHANA • KENYA
MADAGASCAR • MALAWI
MAURITIUS • MOROCCO • NAMIBIA
NIGERIA • SAUDI ARABIA • SOUTH
AFRICA • TANZANIA • UGANDA
UNITED ARAB EMIRATES • ZAMBIA

ASIA

CHINA • HONG KONG
INDIA • INDONESIA • JAPAN
KOREA • MALAYSIA
NEW ZEALAND • PHILIPPINES
SINGAPORE • TAIWAN
THAILAND • VIETNAM

AUSTRALIA

AUSTRALIAN CAPITAL TERRITORY
NEW SOUTH WALES • QUEENSLAND
SOUTH AUSTRALIA • VICTORIA
WESTERN AUSTRALIA

EUROPE

BELGIUM • CZECH REPUBLIC
FRANCE • GERMANY
ITALY • LUXEMBOURG
NETHERLANDS • SPAIN
SWITZERLAND • UNITED KINGDOM

AMERICAS

BRAZIL • CANADA • CHILE
MEXICO • UNITED STATES