Maintaining the Balance Between User Experience and Security

Organisations are seeing a growing preference among employees for using their personal smartphones and tablets for business. Accelerating this trend are inexpensive mobile devices, as well as the launch of the Apple® iPad, bringing tablet computing to life. Employees expect IT to support their personal devices as there is great value in such tools when performing business functions. In an effort to improve employee productivity and end-user satisfaction, many organisations are enabling the use of these devices in their business operations.

The challenge facing these businesses is the security risk of having a variety of mobile platforms in the enterprise environment. How do they begin to ensure sensitive data is not compromised and that vulnerabilities brought about by personal devices are mitigated? Clearly, the answer is no longer to disallow personal devices to access corporate resources. IT professionals can no longer credibly stand in the way of the adoption of mobile technologies – the business drivers are too strong.

Organisations that don’t support personal devices generally fail to enforce policies and ensure governance. As a result, they’re more likely to experience an increased number of security exposures. The odds are that one of those exposures could be catastrophic to the larger business.

An additional consideration is the theft or loss of a personal device containing corporate information and data. Security mechanisms such as remote wipe, pin-based entry and centralised management can satisfy many of your organisation’s basic security requirements.

For a successful mobile implementation, you also need to balance the security requirements of the enterprise with the user’s device experience. Core areas of a successful and mature information security programme include: governance, risk and compliance; mobile policies and security infrastructure.

In this report we’ll discuss some of the challenges and best practices to securely integrate mobile devices into the enterprise. We’ll also cover some security considerations around adaptive security, a critical element of an enterprise mobility framework. We’ll discuss this in the context of an area called Secure User Access, which refers to providing users with access to the network and its resources without compromising corporate data. We’ll review the levels of capability in this discipline and discuss in more depth what elements, at each level, you should be investigating in terms of policy, technology and people.
Contents

Challenges IT faces 01
Addressing the challenges 03
Adaptive security 05
Secure user access 05
A flexible, integrated strategy 06
Challenges IT faces

Theft and loss

By their very portable nature, personal devices tend to be left behind in taxis or restaurants, or are lost due to the carelessness of users or malicious intent of thieves. Now that these personal devices contain sensitive or proprietary company data, such losses or thefts have deeper ramifications.

A study conducted by Carnegie Mellon University found that 42% of data breaches are caused by misplaced or stolen portable devices, and business travellers are the most likely to lose or have a device stolen. According to the study, business travellers lose more than 12,000 laptops per week at airports.

The implications of losing a device can be more catastrophic when you consider the data protection regulations in place today. This is a key concern for organisations that deploy mobile devices.

To help protect the personal and professional data on personal mobile devices, mobile device manufacturers have implemented some basic levels of security features, either through the hardware itself, or through software implementations. For instance, PIN-based entry and device lock is fairly common on most, if not all, devices. In addition, a remote-wipe feature is very common among corporate-issued devices and is effective when the device is no longer in its owner’s possession.

The implications of **losing a device** can be more catastrophic when you consider the **data protection regulations** in place today. This is a **key concern for organisations** that deploy mobile devices.
Data leakage
One place to weigh risk versus reward is downloading and installing productivity, entertainment and social applications, which usually require access to the device’s data or file system and may leave you open to attack. Advanced file or data encryption is usually necessary to protect against active attacks, but encryption alone is not effective when dealing with employee misuse or malicious insider threats. To adequately protect corporate data, you need to control which mobile applications can handle business data and actively restrict data manipulation operations like cut and paste. In some cases, it may be best not to let the device store and handle any local copies of data.

Malware represents another way to leak data and is now increasingly targeting mobile devices. These malware attacks have the ability to root the device and therefore bypass all local security measures. Personal devices are a ripe source for infection. Defending against mobile malware will be an increasingly important IT priority going forward.

Defending against mobile malware will be an increasingly important IT priority going forward.

Legal and privacy implications
Besides the business and data security issues personal mobile devices bring, there are legal implications that organisations must be concerned with. There are many questions to ask when deploying a mobile device policy. Do the very controls that you need to employ to improve security violate local privacy laws? Do you have the legal right to seize the device under certain circumstances? Many of these questions are clearly beyond the scope of security considerations alone.

The question of whether an organisation could be liable for employee misdeeds comes up often. We know employees use personal devices for a variety of tasks not related to work, such as accessing third-party content and media. It’s not uncommon for these devices to contain content that has questionable copyright status. This sometimes poses a legal dilemma to an organisation. Should your mobile policy allow such content on your network? Should you even allow corporate data to co-exist on devices that may contain questionable content?

Obviously, a close relationship between the IT and legal departments is critical when formulating a mobile security policy.
Addressing the challenges
When addressing the security challenges brought on by mobile device proliferation within the corporate network, critical elements include how to provide effective governance, mitigate risk and ensure compliance. This begins with an understanding of information management, or in other words, identifying which data is indeed sensitive or proprietary, and how policy can protect and handle that data accordingly. There should be governance and policy enforcement around whether that sensitive data is even allowed on personal devices or if there is separation of corporate data from personal data on the device. Data protection and risk assessment are important drivers and any compliance enforcement must be aligned with organisational guidelines.

Some level of written policy and procedure that incorporates mobile devices and the handling of mobile data must be in place for organisations to be effective at governance and compliance. You may begin with a basic guideline as to whether employee-owned devices are even permitted to access corporate resources or if only company-provisioned devices are permitted. These policies may revolve around the right for IT to manage any mobile device with access to corporate data, even employees’ personal devices.

The mobile policy needs to indicate which devices will be fully supported, partially supported or not supported at all. For supported devices, there needs to be minimum standards outlined around security measures that can at least be implemented on the device (i.e. encryption PIN codes, remote wipe, etc.). Depending on the device’s ability to support these security measures, you may choose to disallow select devices from accessing the corporate network altogether.

We mentioned previously the desire for users to install a multitude of productivity, entertainment and social applications on their devices. Your policy may have guidelines pertaining to permitted applications, the management of those applications, and a category of disallowed applications. This goes for data handling as well as applications that may compromise the device and its data.

Figure 3: Level of data sensitivity allowed for storage on mobile devices
What is the maximum data sensitivity level that is permitted to be stored on any type of mobile device?

![Data Sensitivity Chart]


Figure 4: Mobile device and data policies
Does your organisation currently have written policies or procedures pertaining specifically to mobile/portable devices or the handling of mobile data?

![Policy Compliance Chart]

Base: 323 respondents in August 2011 and 307 in March 2010
Data: Information Week Mobile Device Management and Security Survey of business technology professionals

Employee acceptance of information technology and mobile usage policies is critical to success. Employees must be made aware of official governance around the privacy of data, and the company’s right to monitor data while in the corporate network, and seize devices in case of investigations. Some organisations implement a forced acceptance of the security policy when the device attempts to connect to the corporate network. Further, employees must be aware of their responsibility to report incidents of loss or theft of their mobile devices.

We discussed earlier how some of these policies may or may not be aligned to government regulations in various parts of the world. Review these matters with your legal department so it can approve the policy or approve it only for certain regions.
Build the security infrastructure

Once the mobile policy has been outlined to align with the governance, risk and compliance drivers of the organisation, it needs to be enforced via technology deployed to mobile devices. These technologies are usually designed according to the device platform in use, and the capabilities of such devices when paired with the deployed management platform. The key here is to deploy technology that balances 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 when taking into account all of the other factors.

The security and management infrastructure you need will depend on what types of policies you employ. For each corporate application or resource that users can access via their mobile device, you must create a technology security checklist. This is critical so that you can work with your counterparts in IT operations to ensure that the right infrastructure, software and processes are in place to enforce or support your security policies. While both the IT department and the employee base can agree that mobile policies and governance are important to overall business success and risk mitigation, 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 appropriately balancing the risk to the organisation.

Different security approaches have different effects on the user experience. A walled garden approach affects user experience, but there is strong data protection; a mobile device management approach doesn’t change the user experience but there is only medium data protection; a virtual desktop infrastructure approach affects user experience and data protection is strong. Ultimately, IT operations want business owners and business users to see them as partners in their mobility needs.

Careful planning and interaction with users will ensure that the policies allow users the level of freedom that they value, while appropriately balancing the risk to the organisation.
Adaptive security

In the first report of this series, Ensuring Mobility Translates into Agility, we discussed using an enterprise mobility framework as a guide when devising your enterprise mobility strategy. Adaptive security is a key element of this framework. Organisations want to determine a security strategy that covers policies, technology and people. While these security strategies vary by organisation, the remit is the same – security for every mobile requirement, device and application.

Security mechanisms across policy, technology and people need to be in place. Elements to consider in this area include governance, risk and compliance. Technology considerations are also in play as we look at connection and device control. With respect to people authenticating and determining the identity of users, it’s critical to ensure approved access to sensitive data and resources on the corporate network.

We’ll explore this operational point of view further – for which we recommend a self-assessment, as it’s a critical reflection point of enterprise mobility. We call this discipline secure user access.

Secure user access

The secure user access competency is an operational competency. It’s an area that focuses on providing users with access to the network and its resources. This access may be based on roles, business needs and security policies. These security policies would usually be aligned with the mobility strategy. For some context, consider if your organisation implements a mobile VPN solution or another means to ensure that the connection for corporate applications is properly encrypted.

Levels of capability

In order to help you work out the levels of your secure user access capability, we’ll describe the possible levels below, including basic, integrated and optimised. With each level of maturity, you can replace reactive mechanisms with more proactive approaches towards meeting an optimised secure user access competency.

Basic capability here indicates that users are actually able to securely access the wireless network using their established network accounts. The use of wireless security protocols like WPA2 should be in place to ensure proper encryption, as well as integration with active directory for authentication. Some level of policy education and awareness is present around e-mail, pin lock and remote-wipe for mobile devices.

An integrated capability goes one step beyond, simply being able to connect to the network. User credentials also ensure that employees can access specific (and correct) applications, systems and data on the network. For example, sales personnel will have access to the sales pipeline information and salesforce.com, but won’t have access to HR reports. Simply put, it’s about role based, ‘intelligent’ access to applications. In addition, as there are multiple entry points, some type of WLAN Intrusion Prevention System should be in place, as well as a basic network perimeter solution (i.e. firewall).

You need to balance security concerns with the user experience of having integrated access to applications, data and systems from any approved mobile device. For example, let’s say you have a field employee who needs to engage the supply chain application and check a product inventory from the field. If they are able to do this, they would then need to place an order on behalf of the customer – also from a mobile location. Already, the positive impact on productivity, timelines, deliverables and customer experience is evident. Organisations at this level understand that security compliance of mobile end points is essential for a complete security strategy implementation.

An optimised capability in this competency would manifest itself in a seamless experience for the user, with a single sign on for all mobile services from any approved device. Users would also be able move between applications across the organisation, grabbing data from different sources and carrying out actions that engage various systems. Such access ultimately allows the user to perform their business function optimally, regardless of their location.

Figure 6: Ability to selectively wipe business data from personal devices

If an employee uses a personal device to access business resources, do you have the ability to selectively wipe (delete) business-related data while leaving personal data intact?

Organisations at this level are consistent in considering network security a high priority. They make the commitment to put in place the necessary tools and technologies to ensure the fastest possible network is also the most secure. This is accomplished using a combination of network perimeter security, a centralised security policy management system, WLAN ‘sniffer’ technology used to detect rogue devices and unauthorised use, and WLAN Intrusion Prevention systems to enforce access policy.

Examples

Below are some examples of mechanisms within a secure user access competency. These are here to help you ascertain where you are in terms of your capability within this competency.

- Field employees can access transactional systems (e.g., product inventory and databases) from mobile devices without compromising sensitive data
- Guests and partners have appropriate access when working on organisational premises
- A network perimeter security solution
- A WLAN Intrusion Prevention System (WIPS)
- Rogue device and unauthorised user detection
- Mobile subscription access is managed per role requirements
- Single sign-on for all mobile services from any approved mobile devices
- Security policies and mechanisms aligned with mobility strategy
- Mobile VPN solution or other encryption solution for remote mobile users

Questions you should ask:

- Can your field staff securely access transactional systems from their mobile devices?
- Do you have network perimeter solutions or WLAN Intrusion Prevention Systems in place?
- Do you have security policies and mechanisms to enforce them for mobile devices and employees?

Some of the examples above can help you determine your desired future state. It's best to think of this in terms of achievable business objectives. Security is considered a high priority and a comprehensive security strategy incorporates all the elements from the previous capability levels – from perimeter and intrusion prevention systems to security policy enforcement and mobile VPN encryption solutions.

When you’re investigating the solutions you’d like to implement to move to a higher maturity level in this area, consider:

- Is it of business benefit for field employees to be able to access transactional systems from mobile devices?
- To improve employee productivity, is it critical to have single sign-on for systems and services across the organisation?
- Is there a need to ensure rogue devices and unauthorised users are blocked from your network via perimeter security or intrusion prevention systems?
- Is there a benefit to enabling mobile users to access, securely and safely, your corporate network remotely?

A flexible, integrated strategy

Organisations are wondering how best to deal with the onslaught of personal mobile devices finding their way into the workplace. As business operation depends increasingly on a mobile workforce, there’s concern that the road to this evolution will be filled with risk and uncertainty. This isn’t necessarily so. All that’s needed is additional focus on the issue to help achieve secure mobility, which will allow organisations to truly realise the benefits that an enterprise mobility strategy promises.

The challenge lies in preserving the user experience while simultaneously and appropriately minimising the risk to the organisation. Consumer technologies are proliferating in the workplace because of the undeniable draw of the consumer experience. Therefore, security and device management policies must not completely inhibit the flexibility and freedom users value otherwise they will simply circumvent those policies which can make matters worse. When it comes to personal mobile devices in the corporate network, you need to somehow strike a balance between mitigating corporate risks and limiting intrusion in the daily work life of your employees. Employee education about safe mobile use practices is critical to promoting an empowered workforce while maintaining organisational security.

One final point to keep in mind is that although there’s plenty of hype in the media around the vulnerabilities of mobile devices and platforms, many of these issues are not new. Consider Trojan viruses or other malicious applications. Security professionals have been warning against the dangers of running untrusted code or opening unknown e-mail attachments for years. The same issues apply for mobile platforms. Mobile devices are fairly similar to laptop PCs. A risk assessment for laptop PCs will tell you where the most prevalent risks are and you don’t necessarily need to aim for much higher security assurance for mobile devices than you do for laptop PCs.

While vulnerabilities affecting mobile browsers pose a serious threat to businesses, one could argue that a greater threat is posed to traditional PCs and laptops by these same issues. It’s important to integrate your mobile and traditional endpoint security approaches. Mobile device security and management should be part of your larger endpoint management strategy. Integrated end point security principles are important, whether a device is located within an individual’s pocket or on top of their desk at the office.

For more information, visit www.dimensiondata.com/enterprisemobility