Strategies for Embracing Consumerization

Microsoft Corporation

Published: April 2011

Abstract

Increasingly, workers want to use their own devices, such as slates, smartphones, and portable computers, for work. For IT to be able to embrace consumerization, risks to the enterprise and its data must be minimized through assessing and understanding user needs and device types.

When consumerization is properly planned and managed, it enables businesses to deliver productivity gains and competitive advantage. This paper describes strategies and best practices that help ensure that corporate assets remain secure and establish new roles for empowered employees and IT as partners.

Microsoft

Copyright information

Contents

1 Executive Summary

The definition of a workplace is changing, and the boundaries between professional and personal lives are being redefined. Users no longer work only within their offices, but often check e-mail late at night and update personal Web sites during the day. The office computer is accompanied by portable computers, slates, and smartphones.

Computing power is now available across a wide range of devices. Consumer devices such as smartphones and slates are now becoming powerful enough to be able to run the types of applications that were traditionally restricted to desktop and portable computers. For many workers, such consumer devices appear to represent the future of computing and empower them to do their job more efficiently. The highly managed IT infrastructure within most enterprises can seem to be a cumbersome and restrictive environment, and does not provide much flexibility. There are so many choices available to consumers that members of the workforce prefer to use their own device at work and pressure IT to support their growing need to stay productive and competitive. The challenge for IT is to be able to embrace consumerization where it is appropriate, while at the same time minimizing risks to the enterprise and to its data. Many newer devices were not initially designed for enterprise use, and careful planning is required to enable the level of management and control that most enterprises require.

As a leader in business and consumer technologies, Microsoft is in a unique position to understand and provide guidance on how best to embrace consumerization responsibly within enterprises. This white paper outlines specific guidance for organizations that are considering whether to adopt the latest consumerization trends.

This paper explores the pressures and the main scenarios of consumerization in the enterprise. It also describes the primary points of consideration, including legal and compliance issues and the technologies. Also presented are examples of different approaches in managing consumerization.

2 What Is the Consumerization Imperative?

Consumerization is the growing trend where business users are making the ultimate choice in what devices, applications, and services they use to get their work done.

2.1 New Workplace Expectations

The workplace environment is changing, due in no small part to advances in mobile devices and remote working technologies. Many workers are spending time working away from the office, perhaps working at home for part of the week, increasingly blurring work-life boundaries.

Many workers are now using their own devices and have the flexibility to work “out of hours,” so there is great potential to improve user productivity, such as during a commute. Technology enthusiasts can be demotivated if they are expected to use older devices that have restrictive software, applications, and network access policies, when they are at work. Recent studies have confirmed this trend. For example, an IDC study that Unisys commissioned found that 40 percent of the time that users spend on their home computer is actually for work. In addition, 50 percent of the time that users spend on their smartphone is also related to work[1].

2.2 Opportunities and Challenges Ahead

Consumerization is the growing trend where business users are making the ultimate choice in what devices, applications, and services they use to get their work done.

By embracing the workforce and empowering it with the latest and greatest technologies, IT can help businesses unleash productivity, reduce costs, and stay competitive. In fact, in a recent study, 83 percent of IT decision-makers characterized the effect of consumerization as mostly positive[2].

However, embracing consumerization is not an easy task and needs deliberate planning from IT. Companies should evaluate how to ensure productivity anywhere, while still protecting data, maintaining compliance, and enabling adequate PC and device management. This all puts pressure on IT to provide compelling solutions for end users while maintaining a secure and well-managed environment.

Examples of such opportunities and challenges can be found in hospitals. Hospitals are major consumers and creators of personal data, and medical staff need access to this data wherever they are on the hospital site. This data access is often provided by mobile data carts, and there is increasing pressure on IT to enable medical staff to use more mobile devices. However, privacy and security requirements, such those contained in the Health Insurance Portability and Accountability Act (HIPAA) and the Health Information Technology for Economic and Clinical Health Act (HITECH), pose special challenges, particularly mobile devices may provide access to data about patients.

---

[1] IDC & Unisys Consumerization of IT Benchmark Study, June 2010

[2] IT Managers Selectively Embrace Consumerization, a commissioned study conducted by Forrester Consulting on behalf of Microsoft, February 2011

3 Factors for Success

There are several key factors that should be addressed so that unmanaged consumer devices can be successfully used within the workplace:

1. **Assess and understand your users**. The first phase involves assessing what consumer-grade applications and devices your employees are using at work today. It will also be helpful to create a profile of your end users and the typical scenarios that they encounter. Depending on the user impact on the business and the needs of users, you may have a different level of tolerance for their use of consumer technologies and a different pace and approach for how to embrace consumerization for different user types in your company. The recent Smart Workforce Segmentation Helps You Better Identify and Meet Worker Needs Study [3], which Microsoft commissioned and Forrester Consulting conducted, can be used as an example to evaluate how other midsize-to-large organizations are distributing technology, what drives these decisions, and how it affects the business.
2. **Assess and understand content and information sensitivity**. Users, and the content that they consume and generate, vary in their level of information sensitivity. For example, some users may deal with sensitive legal issues, whereas others may deal with information that is intended for a public readership. Similarly, some data, such as sales contracts, is highly sensitive and should be kept within securely managed storage. Alternatively, other data, such as marketing brochures, can be shared using consumer technologies such as Windows Live® SkyDrive® without presenting any risks to the organization. As with any technology, adopting consumer technologies for your business should be done responsibly, and that means assessing the risks and then, for your organization, deciding which risks are acceptable and which are not.
3. **Assess and understand your device types and application needs**. Devices are not necessarily good for all tasks:

a. Devices that do not include keyboards, or other rich input mechanisms, may be appropriate for some types of data consumption, but can be poor for data creation.
b. Rich user interfaces on desktop computers and portable computers, including full keyboard and mouse support, in addition to the use of touch or pens on touch-enabled computers and tablets, generally provide the best environment for data creation and manipulation tasks. Windows-based tablets and slates get the full Windows experience

[3] Smart Workforce Segmentation Helps You Better Identify And Meet Worker Needs, a commissioned study conducted by Forrester Consulting on behalf of Microsoft, February 2011

(including Adobe Flash and Microsoft® Silverlight®), customization options, and manageability.

4. **Define the criteria for a successful solution**. Consider what benefits there will be, and how these benefits will be measured.
5. **Use enabling technologies to implement your solution**. Plan on protecting sensitive data, enabling data access and sharing, providing tools for application delivery and access, and providing a centrally managed environment by using enabling technologies such as cloud-based applications and services, in addition to desktop virtualization.
6. **Update your organizational policies**. Your organizational policies should reflect your solution, requiring collaboration beyond IT to include legal, HR, and finance considerations.
7. **Pilot your solution**. Use volunteer users to pilot your solution. They should be highly motivated and keen to work and help create a consumerization strategy for your enterprise. Do not expect to pilot just a single device because such a device is unlikely to be right for all your users—one size does not fit all.
8. **Plan for continuous improvements**. It is unlikely that the first iteration of the program will be perfect.
9. **Ensure that the program drives business value**. The program should not just be a way for particular users to “get cool stuff.” You should identify your user scenarios and productivity needs, and ensure that the program meets these requirements and supports your business objectives.
10. **Provide implementation and development resources**. One thing to consider is to provide sufficient resources to support and develop the delivery of applications and data across multiple platforms. The level of resources that can be allocated will affect the likely costs and timescales for successful implementation of a consumerization project.
11. **Adopt the program**. Roll it out to all employees or to those you have identified as most likely to benefit.

4 What Are the Enabling Technologies?

IT needs to adapt to the new device landscape. Users will increasingly demand more choice in their work devices, which may be met by a personal device or more choice from company hardware. Companies should evaluate new technologies that can enable productive and safe use of consumer devices in the workplace. Such technologies should:

- Protect sensitive data.
- Enable data access and sharing.
- Provide tools for application delivery and access.
- Be capable of being centrally managed.

For most enterprises, consumerization initiatives are unlikely to be realistic options unless most or all of the above requirements can be met. For example, if a user brings his or her own personal portable computer to work, and mixes personal and business applications and data on the same desktop instance, there is a high risk of incompatibilities at best, and data loss and legal issues at worst (such as malicious software or illegal downloads being brought into the workplace).

4.1 Cloud-Based Applications and Services

Cloud computing includes Web-based applications or Web-hosted services, and centralized server farms and data centers, where data is accessed from any type of networked device. A common feature of cloud-based computing is that endpoints are theoretically device-independent; by using the browser on the device as a "universal client," there is no need for client software that is specific to a certain operating system for each type of device that may access the application.

However, for consumer devices, there are several considerations for using cloud applications for corporate data access:

- **Browser requirements**. A key requirement is that browsers on users' devices support the applications. For example, there may be requirements that dictate a particular set of supporting browser versions.
- **Screen size**. There may be screen real-estate issues, particularly for smaller form-factor devices. This can be alleviated to some extent by good design, such as avoiding fixed page sizes.

Microsoft Office 365 and the Office Web Apps are good examples of cloud applications. Office 365 includes online versions of Microsoft Exchange, SharePoint®, and Lync™, and works with Windows-based PCs, Windows Phone 7, and Macintosh computers. Office 365 also includes some functionality that is supported by iPhone, BlackBerry, Nokia, and Android devices. Some phones offer more complete support for Office 365. For example, using Windows Phone 7, you can synchronize SharePoint workspaces to your phone and work with corporate Office documents offline. Other examples of cloud applications include Windows Live Mesh 2011 for synchronizing files across devices and for remote access to PCs, Windows Live SkyDrive for storing and sharing documents and other files, and Windows Intune™ for cloud-based PC management.

4.2 Desktop Virtualization

4.2.1 VDI

In a Virtual Desktop Infrastructure (VDI), Windows-based desktop environments are run and managed in virtual machines on a centralized server. The server then remotely presents the user's desktop to her client computer or other device by using a protocol such as Remote Desktop Protocol (RDP). VDI enables the central management and deployment of user desktops,

but adds the capability for users to access their own personalized desktops, customize their own unique desktop settings, and have administrator rights if necessary (such as for developers).

In contrast to VDI, Session Virtualization enables users to share a single server-based desktop via sessions. You can use Session Virtualization to virtualize the presentation of entire desktops, or just specific applications. You can use Remote Desktop Services, part of Windows Server® 2008 R2, to deliver both VDI and session-based desktops.

4.2.2 Folder Redirection

Folder redirection is one component of a strategy, sometimes referred to as user state virtualization, where user data and settings are stored securely in a central location, and can be cached on the local desktop when users are offline. The primary copy of the data is on the network, so it is easily restored in the case of a lost or stolen PC and the user's settings can be reapplied automatically.

4.2.3 Application Virtualization

Virtualized applications run in a separate, protected, virtualized space, and are not installed in the traditional sense. When organizations deploy virtual applications, they reduce application-to-application conflicts.

The Microsoft implementation of application virtualization is Microsoft Application Virtualization (App-V), which is available as part of the Microsoft Desktop Optimization Pack (MDOP). You can stream App-V applications to users on demand through enterprise software distribution systems such as Microsoft System Center Configuration Manager or through the Microsoft Deployment Toolkit (MDT). Alternatively, you can deploy App-V applications by using stand-alone media. You can manage and service App-V applications centrally, enabling enterprises to update once and assure compliance throughout the organization. Updates are delivered to users seamlessly. Citrix XenApp is a Microsoft Partner solution that extends support for traditional and App-V virtual applications to a wide range of devices, including smartphones and other non-Windows-based devices.

4.3 Choosing the Right Technology

When evaluating technologies, there are three principal questions to ask:

1. **What is the impact on the client device?** A low-impact technology requires no client installation at all, or a lite agent only. A high-impact technology requires one or more agents to be installed on the client.
2. **What level of IT investment is needed?** A low-investment solution uses or extends the current infrastructure, or makes use of cloud technologies. A high-investment solution requires new infrastructure.

3. **How much do you need to control?** You need a low level of control where there are only single applications, or where only baseline security is enabled. You need a high level of control where complete environments are supported.

For example, terminal server computing and VDI both have a low impact on the client, but VDI typically requires more substantial IT investment and control systems. Similarly, management technologies have a high impact on the client, but you can reduce costs by using cloud-based management tools (Figure 1).

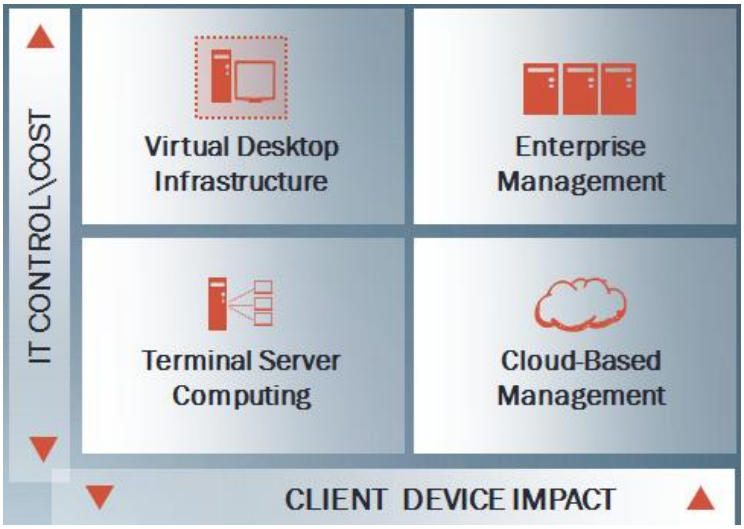

Figure 1. How technologies rate for cost, control, and client impact.

The amount of access that a device has to enterprise resources, including e-mail, documents, and business applications, should depend on the degree to which the device meets organizational criteria. The more the organization trusts the device, the greater the access.

The level of access to information dictates how productive a user can be when working from the device. For example, even unmanaged devices may be permitted access to e-mail and calendar applications, but productivity will be limited unless users are also given access to documents and business applications (Figure 2).

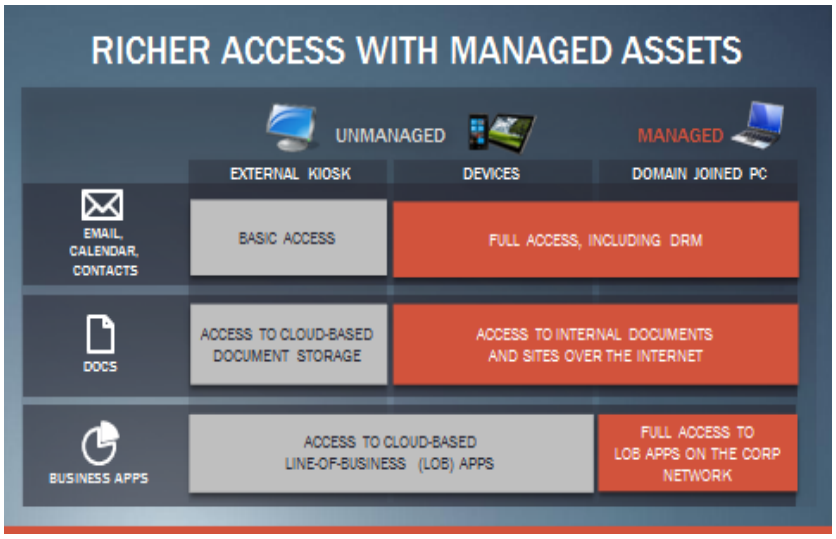

Figure 2. How application access affects productivity for managed and unmanaged devices.

5 Enabling a Diverse Set of Devices

The pressures on IT to enable a diverse set of devices come from several consumerization scenarios.

5.1 Work From Home PC or Bring Your Own Computer

Many organizations are now formalizing their support for home working, and enabling employees to use their home computer for work purposes. In a study of 150 companies, which Microsoft commissioned and Forrester Consulting conducted, 37 percent of IT decision-makers reported that they support some flavor of a Bring Your Own Computer (BYOC) program and an additional 26 percent had plans to do so[4]. Such initiatives may also include financial support for purchasing the computer.

[4] IT Managers Selectively Embrace Consumerization, a commissioned study conducted by Forrester Consulting on behalf of Microsoft, February 2011

Bring Your Own (BYO) describes voluntary agreements whereby employees can use their own computers or other devices in the workplace. In some cases, users are financially supported through a stipend, whereby an employee is provided with a sum of money to purchase a device, and support for a period such as three years. BYO can apply to any device such as any computer (BYOC) or any type of PC (BYOPC). IT should be concerned about the potential complexity of BYO. In the Forrester Consulting study[5], 56 percent of IT decision-makers responded that they are targeting 2011 and 33 percent are targeting 2012 for fully deploying a BYOC program. However, most IT managers have significant work ahead to determine which lines of business or workforce segments should be allowed access to the BYOC program, how the stipend will be extended to users, how to determine corporate policies and the rules of the BYOC program, and how to lock down the security controls of corporate data, applications, and network access.

5.2 Slates and Tablets: Windows-Based or Non-Windows-Based Devices

The increasing choice of form factor for both Windows-based and non-Windows-based devices is also a significant consumerization driver, with a range of slates and tablets becoming available. Users are demanding wider choice, even if IT will be supplying the hardware.

Tablet computers typically include touch screens, in addition to more traditional keyboard and pointer interfaces, and the screen may swivel to hide the keyboard as required. Specialist vendors may produce tablets for specific markets such as industrial, medical, hospitality, and outdoor applications. Slate computers are similar to tablets, but may not have a dedicated physical keyboard; slates may also have a smaller form factor than tablets or more traditional portable computers.

5.2.1 Windows-Based Laptops, Slates, and Tablets

Windows 7 includes a range of new touch features that support both finger gestures on touch screens, and stylus input for more accurate inputs such as handwriting recognition, signature capture, and data entry applications. In certain specialist devices, other Windows-based operating systems may be in use, such as Windows Embedded on point-of-sale (POS) devices and handheld line-of-business (LOB) devices for fleet and warehousing applications. However, you can manage all Windows-based computers through technologies such as System Center Configuration Manager, and they can all be part of an Active Directory® domain.

---

[5] IT Managers Selectively Embrace Consumerization, a commissioned study conducted by Forrester Consulting on behalf of Microsoft, February 2011

5.2.2 Non-Windows-Based Slates and Tablets

Non-Windows-based slates and tablets run a range of operating systems such as Apple iOS, Android, Linux, and others. Although there may be a shared origin in Unix-like systems for some of these operating systems, they provide different user interfaces, and different levels of security and manageability. There are multiple operating systems across this device sector, so it is essential that enterprises adopt a systematic approach to management, otherwise security may be compromised.

5.3 Smartphones

Smartphones are typically defined as mobile phones that provide sufficient computing power to run fairly powerful mini-applications (or apps), and a user-friendly interface to enable interaction with these apps and the phone functionality itself. Smartphones are available for Windows-based and non-Windows-based operating systems.

Windows Phone 7 is the latest Windows-based smartphone operating system. It supports a rich touchscreen user interface, in addition to a range of enterprise features such as built-in SharePoint workspace support for managing Office files, and support for Exchange ActiveSync®.

Non-Windows-based smartphones include devices running Apple iOS, Android, Symbian, and others. Most of these support touchscreen interfaces and, depending on the vendor, specific enterprise management features.

6 What Are the Main Considerations if Enterprises Are to Embrace Consumerization?

Enterprises that are considering their approach to consumerization should review their current and anticipated devices across several key technology and policy areas.

6.1 What Operating Systems and Hardware Need to Be Supported?

Given the wide range of devices that are now available, enterprises should consider whether they are going to be restrictive in their acceptance of consumer or BYO devices, and whether they should set guidelines or more prescriptive rules. Similar considerations will apply for company-owned hardware. In all scenarios, enterprises should look at their proposed support policy, how devices will be updated, and the likely costs for supporting these devices.

6.1.1 Support Policy

Considerations when planning a support policy include:

- How many platforms will be supported, and which versions of each platform will you use?
- Which browsers will you support?
- Will you enforce a standard image? Are there methods for applying standard images?
- Who will be responsible for device support?
- Will you enforce a hardware refresh cycle?
- What peripherals will you need to support?
- What happens when a device is lost or stolen?
- If the device breaks, will there be a backup machine?
- How do you decommission the device at the end of its life?
- What will the minimum device specifications be?

For example, if employees are part of a BYOPC program that stipulates that a purchased laptop must include onsite warranty, you will still need to consider what happens if that laptop has been sent back to the vendor for repair, and the user is temporarily without hardware.

6.1.2 Update Methods

Considerations when planning for update management include:

- How will you manage new versions of firmware or operating systems, or major updates?
- How will you manage security updates?
- Is updating likely to run into cross-vendor issues?
- In the case of phones, do carriers have a veto on operating system updates?
- What is the typical operating system update process for each platform?
- Who provides the updates: the vendor, the carrier, or someone else?
- What security models do they use?
- What is the commitment of the update supplier to timely updates?
- What is the mechanism for delivering the updates?
- What if the hardware vendor stops support (for example, parts are discontinued or back-ordered)?

For example, for Windows-based computers, Microsoft is responsible for all feature and security updates for the operating system and for Microsoft application software. Microsoft maintains 24/7 security issue monitoring and research, issues regular security issue disclosures on blogs and through the Microsoft Security Response Center (MSRC) Web site, and releases security updates on the second Tuesday of each month. For non-Windows-based devices, it is important that you understand the update methods used by device vendors and suppliers.

6.1.3 Costs

Considerations when assessing support budgets include:

- What are the likely costs for maintaining the operating system and hardware?
- Do updates require payment or subscriptions?

For example, updates to supported Windows-based operating systems and applications are free, and this includes major updates through service packs.

6.2 How Will Regulatory Compliance Be Achieved?

A major risk for any enterprise that permits the use of nonstandard devices in the workplace, or for work purposes out of the office, is how to ensure and demonstrate regulatory compliance. This is a particular challenge for more regulated industries such as healthcare, pharmaceuticals, financial services, and government agencies. For example, in the United States, the Sarbanes-Oxley Act (SOX) for corporate governance can have significant compliance requirements.

In considering regulatory compliance, there are several key questions that should be asked:

- **Where is the data?** If data is ever stored on the local device (or copied locally), that data is at risk if the device is lost or stolen, or when employees leave the company. For Windows-based computers, tablets, and slates, you can use BitLocker® to create encrypted local data vaults. You can also use this approach together with policies to ensure that corporate data is only copied down to a local encrypted store, or cannot be copied down at all and is only accessible through remote access tools such as VDI.
- **Are there local laws that need to be considered?** For devices such as smartphones and non-Windows-based slates, it may be important to be able to remotely wipe settings and data on that device if it is lost or stolen. Remotely swiping employees' mobile devices may give rise to legal concerns in some jurisdictions, and enterprises should consult with their lawyers.
- **Will you need to keep a hardware inventory for compliance?** If you need to know exactly what devices are connecting to your network and consuming corporate data, you will need a higher level of management, logging, and inventory procedures. Not all types of device lend themselves to this approach.

6.3 What Applications Will Be Used?

When considering how to provide users with the applications that they need, there are several key questions that should be asked:

- How will you handle line-of-business applications?
- Do all applications need to be available on all devices?
- Does the application vendor support the device?

There are three main approaches to providing applications where there are multiple platforms to support:

1. **Use off-the-shelf applications** for each type of device, and determine any application compatibility issues as soon as possible, because multiple devices and platforms mean that multiple testing is required.
    2. **Use custom development** to create or port applications for each type of device, such as creating Microsoft XNA® or Silverlight 4 applications for Windows Phone 7.
    3. **Use device-agnostic technologies**, such as VDI or the cloud, where it does not matter what type of endpoint device is being used to access the application, and there is no requirement for application support on multiple platforms.

For example, it may be possible to use common applications across all supported devices, as long as the application vendor has a broad device support. Popular applications such as Windows Live Messenger are available for Windows-based desktops, laptops, tablets, slates, and smartphones, and there are versions available for some other platforms. However, many common business applications are not available for all devices, or may have only limited support.

6.4 How Will Applications Be Deployed and Managed?

When considering how to provide users with access to the applications that they need, there are several key deployment and management questions that should be asked:

- How will you deliver applications to users?
- Will you permit user-installed applications, or self-provisioning?
- How will you know what applications you have?
- Will you ensure version control?
- What is the update process and delivery mechanism for typical applications on each platform that you will support?
- How will you manage the application life cycle, including application updates?
- Who provides updates to your applications, and what security models do they use?
- What commitment do your application vendors have to timely updates?
- Is there a way to remove application access to users as roles change, or when users leave the company?
- How will you support audit and compliance reporting?

For example, user-installed applications are a potential problem area unless all Microsoft Software License Terms and licenses are thoroughly checked. Self-provisioning could be manageable if enterprises run their own “app stores” that only offer approved applications, and with the list of available applications customized to specific users.

There are several models for deploying applications, and not all of them include management functionality:

- **Public app stores and marketplaces**. A major issue, especially for handheld devices, is the use of “consumer apps,” which may be available through platform-specific application marketplaces such as the Windows Phone 7 Marketplace. Some of these applications

may actually be business focused, but for platform-specific reasons, may only be available through a public marketplace. Application marketplaces present several challenges for IT:

  - How will an employee buy applications?
  - What identity is used to buy applications: personal or corporate?
  - What is the currency and method of payments?
  - How will the application be updated?
- **Corporate internal app stores**. Increasingly, there are demands for marketplaces that corporate IT can manage. This could be through methods that enable IT to deploy and manage applications within an existing global app marketplace, such as a private marketplace within a public marketplace, or by using a more controlled internal-only marketplace.
- **Push deployment tools**. You can deploy software, including application updates and security hotfixes, over the network by using technologies such as System Center Configuration Manager 2007 R2.
- **Application whitelists**. Whitelists are lists of approved applications; if an application is not approved, it will not run. Being able to restrict the applications that can run on a device can help prevent the execution of potentially malicious software, and ensure that only tested and evaluated applications are available.

6.5 How Will Devices and Data Be Secured?

When considering how to secure devices and data, key questions include:

- How do you control access to sensitive data?
- How do you manage data backup and restore?
- How do you protect data on your network?
- How do you secure data on the device?

For example, unless you can secure data on the device itself, all data should be protected in the corporate data center, or cloud, whatever device is being used. In this way, lost or stolen devices present minimal risk to the enterprise and its data. Therefore, users should be able to use online access to data centers as much as possible, but also be able to use offline access (using secured local data) when they are using roaming devices that cannot be always connected to the corporate network.

Depending on where the data is, and how it is accessed, there are additional specific considerations.

6.5.1 Data on the Local Device

If there are operational or other reasons that dictate that some data may be cached or otherwise stored on the local device, it is essential that the full implications of this are critically assessed,

and procedures put in place to mitigate any risk to the enterprise, such as in the event that the device is lost or stolen.

Key issues to consider for all devices that may store sensitive data are:

- Can local data be encrypted?
- Are there protected data storage areas on the device?
- Does the device support removable storage devices such as SD cards or USB drives?
- If removable storage is available, can access to this storage be disabled?
- What local data and settings should be backed up, and how?
- How do you protect against malicious software?

For example, using VDI for accessing corporate resources helps to keep a clear, protective barrier between potentially infected user devices, such as smartphones or slates, and the enterprise. The virtual desktop itself is kept within the firewall, and as long as the device's VDI client does not permit local data to be copied or transferred to the virtual desktop, any malicious software on the client cannot affect network resources.

Effective strategies for dealing with malicious software are particularly important on devices that may hold local copies of sensitive data or be running local applications that access corporate resources. For example, there should be systems in place to deal with endpoint security, such as antivirus and rootkit protection. For newer devices, there can be an initial period when it appears that the device is not a target for malicious software. However, as the number of such devices increases, the prevalence of malicious software inevitably also rises. Antivirus vendors are reporting that mobile malicious software is becoming an increasing problem, due both to the numbers of smartphones and similar devices, and the fact that most are now connected to the Internet.

6.5.2 Data in the Cloud or Corporate Data Center Only

Wherever possible, data should reside within protected clouds or data centers. In this way, data should not be exposed on the local device.

Key issues to consider where data is stored in the cloud or data center are:

- How will reliable network access to this data be delivered?
- Are there specific network requirements such as requirements for firewalls?
- Do access technologies, such as Windows Media® Digital Rights Management, need to be supported?

For example, if the device is using a cloud-based application, such as an Office Web App, all data can be kept in the cloud storage. If the enterprise has implemented policies, such as rights management, to control who can access and edit documents, for example, these policies can be applied in the cloud application and will be enforced locally at the client. One way of doing this is by using Office Web Apps through a Web browser, which will automatically respect online rights management policies, regardless of the device being used.

6.5.3 Enabling Network Access

All BYO devices should be treated as untrusted devices when they are connected to corporate networks, in the same way as devices such as home computers that are using remote access. One approach is to configure your infrastructure so that such devices are not able to connect to trusted resources, even when they are used within the workplace. One way of doing this is by using switch-level protection to prevent untrusted devices from being physically plugged into the corporate local area network (LAN).

Key issues to consider when planning for enabling network access are:

- What technologies are in place for enabling network access?
- Can the network infrastructure be configured to permit untrusted devices?
- Are there any network access limitations on any proposed devices?

For example, for mobile devices, there are several common approaches for providing network access to corporate resources:

- **Virtual private networks (VPNs)**. VPNs are one way to access corporate resources, through a secure, private channel from the endpoint. For Windows-based computers, and for other platforms such as Macintosh and Linux, the ability to support multiple VPNs is typically built in to the operating system. However, for smaller form-factor devices, there may be limited support for VPNs, or the ability to configure only a single VPN configuration.
- **Reverse proxies**. Reverse proxies are used as an alternative to direct connections to endpoints. They provide an extra protective layer between the corporate resources, such as Exchange servers, and external devices. Reverse proxies enable Secure Sockets Layer (SSL) encryption and acceleration services to be offloaded from the endpoint service, and also provide load balancing where the reverse proxy server can distribute all of the traffic that is targeted for a single URL to a group of endpoint servers.

6.5.4 Enforcing Network Security

There are various methods that can be used to restrict network access to compliant devices only. Without such controls, it is difficult to ensure that a compromised device, such as a smartphone, does not then also compromise the corporate network when it is connected.

Key issues to consider when planning for network security are:

- Does the device support any access protection technology?
- What mechanisms will there be for users to get their own devices into compliance?

For example, on Windows-based computers, you can use network access protection (NAP) to control access to network resources based on a client computer's identity and compliance with corporate governance policy. If a client is not compliant, NAP provides a mechanism to automatically bring the client back into compliance and then dynamically increase its level of network access. For BYO devices, it is important to consider whether tools, such as Web portals,

can be provided so that users can deal with operating system and policy updates themselves if their device is identified as being out of compliance.

6.5.5 User Authentication

User authentication procedures first confirm the identity of any user who is trying to access protected resources, and then enable user access to permitted resources.

Key issues to consider when planning for user authentication are:

- On consumer devices, how will multiple identities be managed?
- Does the device support user names, personal identification numbers (PINs), and passwords?
- Does the device support smart cards or biometric authentication methods?
- Is multifactor authentication supported, such as user name and password plus certificates?

For example, a user's personal identity, such as his Windows Live ID, and his work identity, such as his domain logon and corporate e-mail address, may affect which applications can be run if a personal certificate is required. There is also the issue of personal and corporate data that may coexist on the same device, but be subject to separate identities for data access controls. Where VDI solutions are used to access server-hosted virtual desktops, you can use Active Directory to identify active users on the network, in the same way as for domain-joined regular computers. Devices, such as non-Windows-based slates, do not support this unless using a VDI solution.

On larger form-factor devices, such as Windows-based computers, you can use smart cards to verify user identity before any network connection can be made. Smaller devices may not have the necessary hardware support for smart cards or biometric scanners.

6.6 How Will Devices Be Managed?

The range of devices that consumerization may introduce into the workplace presents IT with several management-related challenges. For corporately owned computers, a high level of device management can be achieved. In other cases, only limited management may be possible.

The key management issues include:

- What devices are in use, and who is using each device?
- What applications are on each device, and are these applications supported and licensed?
- Is each device up to date with updates, fixes, applications, and so on?
- In the event of security problems, are mechanisms available for rapidly closing such breaches?
- Can security policies, such as password complexity, be easily enforced?
- What support, or remote assistance, is required, and is this required 24/7?
- What tools are available for devices that rarely connect to the corporate LAN?

For example, there are several types of technology that you can use to impose some form of management on consumer devices:

- Cross-platform tools such as Exchange ActiveSync.
- Windows-based tools such as System Center Configuration Manager and Windows Intune.
- Non-Windows-based tools such as the Apple iPhone Configuration Utility and Mobile Device Management (MDM) application programming interfaces (APIs).

6.7 How Will User Responsibilities Be Managed?

Successful management of consumerization is not just about technology; effective organizational and employment policies also have their place. For example, if BitLocker or other third-party encryption is required as part of a precondition for connecting a device to the corporate network, the legal implications of encrypting data on a personal system should first be fully investigated.

It may be useful to include clauses in employment policies on the use of employees' own devices, defining what rights the employee has and what rights the employer has. These policies could include:

- User agreement to accept device requirements such as password enforcement.
- Any rights the organization has to wipe devices remotely, such as if the device is lost or the user leaves the company.
- Any commitment the organization has to supply temporary loan devices if a user's BYO device is broken. Even if a warranty is required, there will often be a period of unavailability.

The enterprise should set out clear rules so that only when employees sign the relevant document or contract do they get access to corporate resources through their supported devices.

7 Solutions for Managing Consumerization in the Enterprise

This section describes several example solutions for managing consumerization in the enterprise, within highly managed corporate environments and in more dispersed organizations, and for both Windows-based and non-Windows-based devices. Figure 3 shows how the key Microsoft technologies in these solutions rate in terms of typical costs, level of required control, and client impact.

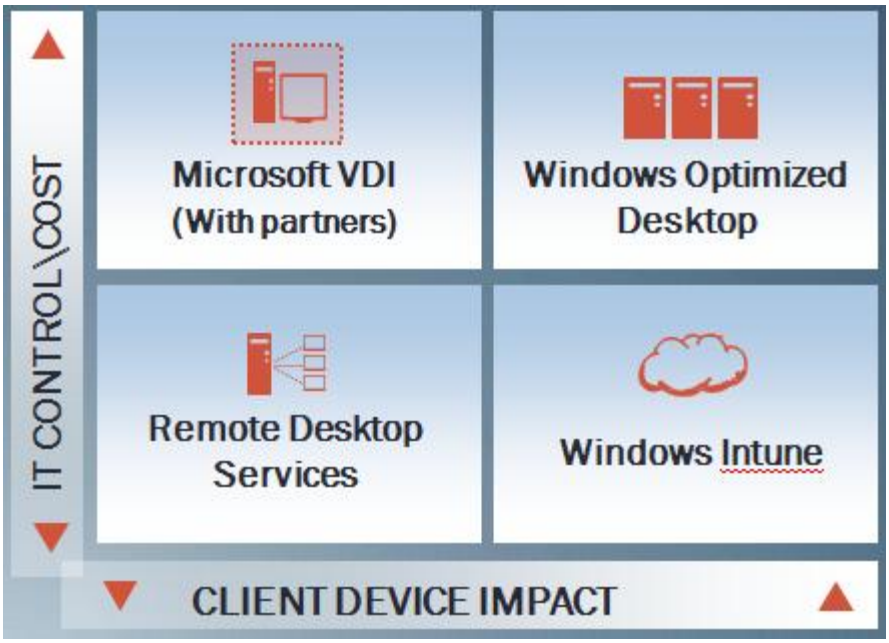

Figure 3. Key Microsoft enabling technologies rated for costs, control, and client impact.

7.1 PCs and Slates

The best approach for managing BYO PCs, Macintoshes, and slates in the enterprise depends on the types of device that IT is expected to manage.

7.1.1 Windows Optimized Desktop

The Windows Optimized Desktop combines Microsoft solutions for desktops through to data center management across physical and virtual environments. At the base level is client infrastructure, including Windows 7 as the desktop operating system, Windows Internet Explorer® 8 as the browser, and MDOP. The infrastructure for Windows 7 Enterprise and Windows Server 2008 R2 supports client features such as BranchCache™ and DirectAccess. In addition, through Hyper-V™, it supports VDI environments.

Management tools in System Center and security technologies in Microsoft Forefront® support the client and server components. Management tools, such as System Center and MDOP, provide the security, access, and application optimization tools for locally deployed systems, and for systems and applications that are hosted on-premises in the data center:

- **Application management.** In Windows Optimized Desktop environments, you can use a managed deployment approach, using software such as System Center Configuration Manager or Microsoft System Center Essentials, to deploy Windows-based applications to Windows-based computers. Using this approach, you can deploy applications to large

numbers of computers at the same time. For Windows-based PCs, slates, and tablets, the AppLocker™ feature in Windows 7 Enterprise enables administrators to create a whitelist of approved programs that can be selected individually by file hash, in groups by location, or in groups by publisher (signed by the publisher's certificate). After Windows 7 clients using Group Policy have downloaded AppLocker rules, only the whitelisted applications are permitted to execute.

- **Local data security.** For Windows-based computers, BitLocker Drive Encryption is a data protection feature that uses a protected storage area at the volume level. BitLocker is integrated with the operating system to address threats of data theft or unauthorized data access, primarily from lost or stolen portable computers. BitLocker is available in Windows 7 Ultimate and Windows 7 Enterprise. In more managed environments, you can use the Encrypting File System (EFS) to protect specific files and folders on portable computers, desktops, and servers. EFS encrypts the contents of protected documents and enables users to choose the documents that they want to encrypt.
- **Removable storage**. In Windows 7 Enterprise, BitLocker To Go™ extends BitLocker Drive Encryption protection to USB removable storage devices.
- **Backups**. Where data is stored and manipulated on the local device, it is essential for this data to be protected and backed up. For Windows-based tablets and slates, you can use the built-in Windows 7 backup tools to back up data to USB and other external devices. Where devices have regular access to corporate networks, you can use technologies such as Microsoft System Center Data Protection Manager 2010 for rapid backups where only block-level changes are copied. For mobile Windows-based computers, System Center Data Protection Manager 2010 can also take snapshot backups offline that are automatically synchronized to central backup servers when they are next connected to the corporate LAN. However, where, for example, a portable computer is used for both work and non-work tasks, the challenge is how to back up just enterprise data and not to use corporate resources to back up non-work-related information.
- **Network access**. Microsoft Forefront User Access Gateway (Forefront UAG) can provide reverse proxy services for Exchange and Internet Information Services (IIS) servers, in addition to doing so for other corporate services. For Windows Phone 7, for example, data transmission is encrypted by using 128-bit or 256-bit SSL encryption, through reverse proxies that are hosted by Forefront UAG.
- **Network security**. On Windows-based computers, NAP provides a range of enforcement options:
  - **IPsec Enforcement**. Unless the computer is compliant, no IPsec communications with other computers are permitted.
  - **802.1X Enforcement**. Unless the computer is compliant, only limited communications across any 802.1X-authenticated network connection, such as to an authenticating Ethernet switch or an IEEE 802.11 wireless access point (AP), are permitted.

- **VPN Enforcement**. Unless the computer is compliant, only limited communications over a VPN connection are permitted.
- **DHCP Enforcement**. Unless the computer is compliant, only a restricted IPv4 address will be leased to the computer. Such an address only permits access to a restricted network.

For more information about NAP, see the Network Access Protection page at http://technet.microsoft.com/en-us/network/bb545879.

Other approaches to ensuring compliance include management tools such as System Center Configuration Manager, which you can use to identify devices that have no or limited encryption, no antivirus, or do not have up-to-date operating system or application updates.

- **User authentication**. All Windows-based computers use user names and passwords. For Windows-based computers, you can use local or domain policies to set required password complexity and password renewal periods.

7.1.2 Windows with Windows Intune

For organizations that do not have the resources or infrastructure to support the complete Windows Optimized Desktop strategy, Windows Intune can help deliver the management and security essentials. Windows Intune is a cloud-based management solution that brings together Microsoft cloud services for PC management and endpoint protection with upgrade rights to Windows 7 Enterprise and future versions of Windows. Using Windows Intune, IT can give workers the best Windows experience with the latest Windows-based operating systems and keep those PCs current and protected with the Windows Intune cloud service.

Windows Intune delivers management and protection through an easy-to-use, Web-based console. IT gets immediate insight into the user's PC environment and can view the status of updates and malicious software, alerts, security policies, hardware and software inventory, and more. All that is needed is an Internet connection and the Windows Intune client installed on each managed PC.

Windows Intune can help to deliver the essentials of management and protection—updates, endpoint protection, and asset inventory—to unmanaged and lightly managed devices. Windows Intune does not require Windows-based computers to be part of an Active Directory domain.

For Windows-based portable computers, slates, or tablets, Windows Intune provides an effective, cloud-based management and protection solution. For users who are part of a BYOPC program, Windows Intune includes rights to deploy Windows 7 Enterprise on that PC in addition to managing and protecting that PC with the cloud service. The underlying license requirement to purchase and deploy Windows Intune is Windows 7 Professional, Windows 7 Business, or higher editions. Windows Intune supports PCs only, and the following versions of Windows editions:

- Windows 7 Enterprise, Ultimate, and Professional
- Windows Vista® Enterprise, Ultimate, and Business
- Windows XP Professional with Service Pack 2 (SP2) or later (SP3 is recommended)

7.1.3 VDI

For devices that cannot provide the full Windows 7 experience and security environment, you can use a VDI-based strategy to enable secure access to a server-hosted, Windows-based desktop. This approach is the most effective one for non-Windows-based portable computers and slates, such as Macintoshes, iPads, and Linux-based netbooks. However, the VDI approach can also be useful where employees bring their own Windows-based portable computers into the workplace. In this case, VDI is used to deliver a secure enterprise desktop, with all personal data and software being kept out of the corporate network.

One example solution includes technologies from Microsoft and Citrix. Microsoft VDI suites provide the base platform for the desktop infrastructure and use:

- **Hyper-V** as the virtualization layer.
- **App-V** as the application virtualization platform.
- **Microsoft RemoteFX™** for a rich user experience.
- **System Center** technologies to manage the infrastructure.

Citrix XenDesktop manages desktop delivery, in addition to providing a rich user experience across the wide area network (WAN). You can use Citrix Receiver to extend virtual desktops onto devices such as non-Windows-based tablets and smartphones; the screen is updated on the device, but corporate data is kept secure in the data center. You can use VDI technologies, such as Citrix Receiver, to touch-enable any Windows-based application so that it can be used on non-Windows-based devices.

Considerations for using a VDI solution such as the Microsoft-Citrix solution are:

- **Storage optimizations**. When converting or preparing desktops to use as virtual desktops, it is important to look at what performance optimizations are available, such as configuring appropriate storage block sizes on the server to maximize server disk performance.
- **The number of images to support**. When streaming operating system images by using Citrix Provisioning Services, it is often most efficient to use one or two standard images, which are then streamed to multiple users.
- **E-mail configuration**. When using Microsoft Outlook®, do not use Cached Exchange Mode, because the desktop is in the data center and is never offline in a VDI-type scenario. (If the ICA connection is broken, you lose access to the desktop, but it is still online as far as Exchange is concerned.)
- **Bandwidth requirements**. A lot more bandwidth is required for full VDI (XenDesktop) solutions than for solutions that only use virtualized applications, such as Citrix XenApp, Microsoft App-V, or Microsoft RemoteApp. This is because there is typically a lot more idle time, and lot lower average utilization for virtual applications than for full virtual desktops.

For more information about using Hyper-V and XenDesktop, see TechNet Virtual Lab: Implementing Citrix XenDesktop 4 on Hyper-V R2 at https://cmg.vlabcenter.com/default.aspx?moduleid=281742e3-2613-42da-bd58-2c3578f039b4.

7.2 Smartphones

There are various ways to manage smartphones in the enterprise. For example, you can use Exchange ActiveSync to manage a wide range of Microsoft and non-Microsoft devices. Exchange ActiveSync is a Microsoft Exchange synchronization protocol that is optimized to work over high-latency and low-bandwidth networks. The protocol, which is based on HTTP and XML, enables devices to access information, such as e-mail, calendars, and contacts, on an Exchange server, in addition to providing management tools through Exchange ActiveSync mailbox policies and other tools. For example, Windows Phone 7 supports Exchange ActiveSync management policies, such as requiring passwords and enforcing different levels of password strength, in addition to the ability to remotely wipe the device and restore its original factory settings after multiple failed attempts to unlock it. Management based on Exchange ActiveSync is an industry standard for smartphones and other small form-factor devices, and is supported by platforms such as Apple iPhones and iPads, Android, Symbian, and Palm.

Common smartphone management requirements in the enterprise include:

- **Remote device wipe**. Exchange Server 2010 enables you to send a command to a mobile phone that will perform a wipe of that phone. This process, which is known as a remote device wipe, clears all Exchange information that is stored on the mobile phone to clear data from a stolen phone or clear a phone before assigning it to another user.

For more information about remote wipe in an Exchange 2010 environment, see Perform a Remote Wipe on a Mobile Phone at http://technet.microsoft.com/en-us/library/aa998614.aspx.

- **Password locking**. This Exchange ActiveSync policy is used to require users to lock their mobile phones by using a password. You can also enforce a variety of policy settings that guide the usage of mobile phone passwords. As long as an Exchange ActiveSync mailbox policy has been created, the settings that you can configure include the following:
  - Enforcing an alphanumeric password.
  - Enabling password recovery.
  - Requiring encryption on the mobile phone.
  - Specifying a minimum password length.
  - Specifying a period of inactivity before you must re-enter a password on a mobile phone. This is known as device password locking.

For more information about password locking in an Exchange 2010 environment, see Configure Device Password Locking at http://technet.microsoft.com/en-us/library/bb125004.aspx.

- **Idle time-out value**. Direct Push Technology uses Exchange ActiveSync to keep data on a Windows-based phone, or other phone using Exchange ActiveSync, synchronized with data on an Exchange server. On firewalls, a network idle connection time-out indicates how long a connection is permitted to live without traffic after a Transmission Control

Protocol (TCP) connection is fully established. You must correctly set this time-out value to allow the Exchange ActiveSync heartbeat interval and the enterprise session interval to communicate effectively. If the firewall closes the session, mail would be undelivered until the client reconnects, and the user could be unsynchronized for long periods of time. Microsoft recommends that organizations set time-outs on their incoming firewalls to 30 minutes. For more information, see Understanding Direct Push and Exchange Server 2010 at http://technet.microsoft.com/en-us/library/ff459598.aspx.

- **Exchange ActiveSync Autodiscover settings**. You can use the Autodiscover service to provision mobile phones for users when the user's e-mail address and password are supplied. The ability to use the Autodiscover service depends on the mobile phone operating system. Not all mobile phone operating systems that support synchronization with Exchange 2010 support Autodiscover. For more information, see Configure Exchange ActiveSync Autodiscover Settings at http://technet.microsoft.com/en-us/library/aa998277.aspx.
- **Troubleshooting Exchange ActiveSync**. The online Exchange Remote Connectivity Analyzer is an essential tool for troubleshooting Exchange ActiveSync, and tests issues such as e-mail settings and synchronizations. For more information about the Exchange Remote Connectivity Analyzer, and to use the tool, go to https://www.testexchangeconnectivity.com/.

The best approach for managing smartphones in the enterprise depends on the types of phone that IT is expected to manage.

7.2.1 Windows-Based Phones

Windows-based phones are designed to support specific enterprise management features:

- **Local data security**. Some customers require smartphones to encrypt data at rest on the device. Windows Phone 7 uses a least-privileged security model, including application certification and sandboxing with isolated storage to protect data. Application developers can make use of cryptographic APIs to encrypt application data if they want to. Windows Phone 7 prevents users from transferring files from or to a PC by using a USB connection. Windows Phone does not support removable memory cards, preventing information from being transferred to or read on a PC. You can only use the Microsoft Zune® software to synchronize media files (such as music, picture, and video files) with a PC. When a Windows-based phone is lost, an administrator or the end user can wipe it remotely, or the phone will wipe automatically when a wrong PIN is entered multiple times.
- **Removable storage**. For Windows Phone 7, removable data storage cards are not supported. Windows Phone 7 devices come with a minimum of 8 gigabytes (GB) of data storage. If an original design manufacturer (ODM) has designed a Windows Phone device with an SD card, Windows Phone protects the data by locking the card. To “lock” the card, a 128-bit key is used and stored in the built-in memory of the phone to uniquely

pair the card with the phone. The result is that if the card is removed from the phone, the SD controller will prevent access to the card unless the correct 128-bit password is supplied. SD cards that are paired with a specific Windows Phone device can no longer be used in other phones or a PC.

For more information about Windows Phone 7 security, see Windows phone capabilities security model at http://blogs.msdn.com/b/jaimer/archive/2010/04/30/windows-phone-capabilities-security-model.aspx.

- **Backups**. For Windows Phone 7, the Zune software is used to back up media files and SharePoint synchronization is used to ensure that Office documents and other documents are copied back to enterprise servers. On Android devices, personal data, such as phone contacts, is automatically backed up through synchronization to the user's Google account, but call records and application data are not. You can use third-party applications to back up this data. For devices using Apple iOS, you must manually back up all personal data to a computer by using iTunes software.
- **Protection against malicious software (also called malware)**. Antimalware tools for smartphones are still not mainstream. However, Windows Phone 7 uses a least-privileged security model, including application certification and sandboxing to prevent malicious software attacks.
- **User authentication**. All Windows-based computers use user names and passwords, and Windows Phone 7 supports device security by using passwords and PINs. For smartphones, you can use Exchange ActiveSync policies to ensure that appropriate passwords or PINs are used.
- **Device management**. To manage Windows Phone 7 devices, IT can make use of Exchange ActiveSync for policy support, and to manage e-mail and document access. It is important to note that at present, Windows Phone 7 devices only support a subset of the Exchange ActiveSync policies that are available with Exchange 2003 SP2, Exchange 2007, and Exchange 2010. Currently, Windows Phone 7 supports the following Exchange ActiveSync policies:
  - **Password Required**. (This is the only policy available on Exchange 2003 SP2.) Requires the user to set a device-locking PIN before the phone starts synchronizing e-mail, calendar, and contact information with an Exchange server.
  - **Minimum Password Length**. Sets the minimal number of numeric characters in the PIN.
  - **Idle Time-out Frequency Value**. Defines the time before a phone locks when not in use.
  - **Device Wipe Threshold**. Defines the number of times that a wrong PIN can be used before the phone wipes and resets to factory settings. (In addition, remote device wipe can be initiated either by a user through Outlook Web App or by an Exchange administrator.)
  - **Allow Simple Password**. Can be used to prevent the user from using a simple PIN such as 1111.
  - **Password Expiration**. Sets the validity period of a PIN, after which the PIN has to be renewed.

- **Password History**. Prevents the user from reusing the same PIN repeatedly.

For more information about using Exchange ActiveSync policies with Windows Phone 7, see Exchange ActiveSync Considerations When Using Windows Phone 7 Clients at http://social.technet.microsoft.com/wiki/contents/articles/exchange-activesync-considerations-when-using-windows-phone-7-clients.aspx.

For more information about Exchange ActiveSync policies that are supported on Windows Phone 7, see Exchange ActiveSync Client Comparison Table at http://social.technet.microsoft.com/wiki/contents/articles/exchange-activesync-client-comparison-table.aspx.

Exchange 2010 includes a new Allow/Block/Quarantine (ABQ) feature. Where Exchange ActiveSync policies enable administrators to limit device access by capabilities, the ABQ list enables access to be controlled by device type.

For more information about the ABQ list, see Controlling Exchange ActiveSync device access using the Allow/Block/Quarantine list at http://msexchangeteam.com/archive/2010/11/15/456931.aspx and Understanding Mobile Device Management at http://technet.microsoft.com/en-us/library/ff959225.aspx.

7.2.2 Non-Windows-Based Phones

The enterprise management features supported by non-Windows-based phones varies from vendor to vendor. For example, many devices support management based on Exchange ActiveSync policies, but not all non-Windows phones work with all Exchange ActiveSync features. In addition, the version of Microsoft Exchange is important, with more support for non-Windows-based phones being provided by Exchange ActiveSync 12.0 (Microsoft Exchange Server 2007) and earlier Exchange versions. However, as long as your device/Exchange combination is supported, this means that you can use procedures such as the Exchange remote wipe procedure for any smartphone, not just Windows Phone 7 devices.

For more information about Exchange ActiveSync policies that are supported on non-Windows-based phones, see Exchange ActiveSync Client Comparison Table at http://social.technet.microsoft.com/wiki/contents/articles/exchange-activesync-client-comparison-table.aspx.

If appropriate Exchange ActiveSync policies are not available for the smartphones that must be supported, you will need to consider vendor-specific or third-party tools:

- **Application management**. There are various approaches to the management of applications on Linux-based and Android slates and smartphones. For example, tools are available that can enable or disable application installations, provision applications and application updates, restrict network access for applications, and collect application inventory data. It is important that enterprises set out minimum requirements for application management before considering which tools and methods may be appropriate

for enterprise needs. On Apple iOS devices, the use of custom or in-house applications can be controlled with a provisioning profile. Users must have the provisioning profile installed to execute the application. You can install or revoke provisioning profiles over the air by using MDM solutions. Administrators can also restrict the use of an application to specific devices.

- **Local data security**. Recent Apple iOS devices include encryption, and Android devices support encryption through third-party applications.
- **Device management**. Apple iOS devices support some, but not all, Exchange ActiveSync policies, depending on the version of Exchange. Apple also provides the iPhone Configuration Utility, which is used to create XML configuration profiles that can be distributed to phone users. These profiles include similar policy settings to Exchange ActiveSync, such as passcode requirements. Larger enterprises can also make use of MDM APIs to create their own management tools for functions such as remote wipe and other policies that are similar to Exchange ActiveSync policies. In addition, larger enterprises can use MDM for other functions such as alerting IT when the phone becomes liable for international roaming charges, turning off cameras, verifying strong passwords, and collecting detailed asset information. MDM tools require a client to be installed on the device, and there are now third parties that supply management tools based around MDM and Exchange ActiveSync functionality. For Apple iOS devices that do not use Exchange ActiveSync or other enterprise tools, you can use the consumer-focused iPhone MobileMe service to locate missing devices on a map, display a message on its screen, remotely set a passcode lock, and initiate a remote wipe to delete personal data.

On Android devices, the Google Apps Device Policy enables administrators to remotely wipe data on lost or stolen devices, lock idle devices, and manage passwords for devices running Android 2.2 or later. Administrators can also enforce data security policies such as:

- Requiring a device password on each phone.
- Setting minimum lengths for more secure passwords.
- Requiring passwords to include letters and numbers.

Device policy management APIs enable developers to create applications to control features, such as managing e-mail and VPN accounts, and installing certificates. However, this is also a potential problem area if important security features are dependent on each phone vendor and the API features that they support.

7.3 Microsoft Can Help

Microsoft has always been interested in delivering software that empowers people at work and at home. This commitment is deeply rooted in Microsoft's original mission statement: "A PC on every desktop and every home." With over a billion customers across the globe today, Microsoft delivers solutions that power the world's largest enterprises, schools, government offices, and small businesses, in addition to hundreds of millions of homes.

Microsoft delivers consumer experiences across the PC, phone, and television: Windows 7, Hotmail®, Windows Live Messenger, Bing™, Xbox®, Xbox LIVE®, and Kinect™ are current examples.

For enterprises that have fully managed infrastructures, the Windows Optimized Desktop, which includes **Windows 7 Enterprise** and the **Microsoft Desktop Optimization Pack**, delivers the key capabilities that enterprise customers have asked for. The Windows Optimized Desktop enables user productivity and gives users anytime, anywhere access to the information that they need to get their work done. In addition, it provides tools for IT to support its business securely, protect corporate data, achieve cost efficiencies, and take advantage of the virtualization trends in the client computing arena.

For businesses that have less managed infrastructures, Windows Intune provides cloud-based management and protection technologies for Windows-based desktops, portable computers, and slates. Windows Intune enables essential tasks including updates, endpoint protection, and asset inventory to be performed on any device that has an Internet connection.

8 Summary

Workers increasingly want to be able to use their own devices, such as slates and smartphones, at work, and many are also prepared to purchase their own portable computer or other device as part of a BYO program.

IT must be able to embrace consumerization where it is appropriate, while at the same time minimizing risks to the enterprise and to its data. By assessing and understanding your users, in addition to the devices that they want to use, you can help ensure that consumerization benefits your business, and that these benefits can be measured and evaluated.

Embracing consumerization enables businesses to deliver productivity gains and competitive advantage. Consumerization becomes a major opportunity when the strategies that are described in this paper are followed, ensuring that corporate assets are secure and establishing new roles for empowered employees and IT as partners. Microsoft has a range of enterprise-ready solutions that can help you address your users' needs around consumerization, from deployments of Window Optimized Desktop, through cloud-based management using Windows Intune, to Windows-based and non-Windows-based smartphones.