V E N D O R S P O T L I G H T

Balancing Risk and Productivity – How to Secure Mobile Proliferation

March 2011

Eric Domage, Megan Dahlgren, Phil Odgers

Introduction

Mobility is no longer the exclusive realm of the corporate executive. As a result, all stakeholders (employees, clients, partners) who want to connect to corporate networks, systems and applications are using a variety of mobile and remote access devices to do so.The prolifertation of mobile devices and the trend of users bringing in their own networked devices has created a security threat for IT and network administrators. To address the security risks posed by opening networks to unmanaged devices, IT organisations will need to implement a comprehensive security policy and manage remote access to the network and key applications. Most IT organisations use a combination of approaches, but with each layer of mangement and security there is added complexity.

By 2014, IDC expects more than 28% of all mobile devices shipped worldwide to be converged mobile devices with Internet access. The growth of mobile broadband and access to applications is driving mobile subscriber growth — over 1.3 billion mobile phone subscribers will be added by 2013 to reach 4.9 billion subscribers. The emergence of connected devices such as embedded laptops and a plethora of M2M devices will also increase mobile Internet access to corporate networks and systems, adding more weight to the question of how to manage the risks posed by mobility.

Consumerisation[1] is another increasingly critical topic for IT decision makers. IT managers and CIOs are facing an explosion of popular devices and applications in their enterprises, which they are struggling to control from a security policy, management and cultural perspective. IDC believes that consumerisation will be an unstoppable trend over the next five years, and IT managers therefore need to make key decisions and adopt a coherent strategy in order to manage its impact.

Ubiquitous Mobility

Mobility facilitates the extension of IT resources and application availability to **anytime**, **anyplace**, **anyway**. Mobility has become ubiquitous with efficiency and has moved from hype to reality. It is now critical to businesses and organisations' operations, productivity and competitiveness. As with any critical business enabler, mobility requires security, compliance, and scalability to maintain its effective contribution as an enabler of ICT innovation.

One of the principle missions of the European Commission, for example, is to promote the competitiveness of ICT industries and services and to support the uptake of ICT and ebusiness practices among European enterprises, especially mobility. According to the EU Commission, ICT investment helps to increase labour productivity and enables firms to increase their overall efficiency and makes them more competitive.[2]

[1] According to IDC, the consumerisation of IT can take two forms: **1)** Employees applying pressure to bring and connect their personal devices (e.g., Smartphones, USB sticks, mini notebooks, computers, and tablet PCs) to the corporate network to use as productivity tools. **2)** The use of Web 2.0 social applications such as LinkedIn, Facebook, and Twitter in a business context. Social media is increasingly being used directly from the workplace or accessed using corporate resources while working remotely for both personal and business purposes.

[2] Source: http://ec.europa.eu/enterprise/sectors/ict/competitiveness/index_en.htm

With the full support of the European Commission and many other government organisations, massive investments are being made in network upgrades and performance. This will only increase the trend for users to expect ubiquitous access to applications and resources from anywhere at anytime.

What is the Impact of Mobile Proliferation and the Consumerisation of IT?

IDC has isolated five key areas where consumerisation will have the most impact on the enterprise:

- **Cost**: Supporting new devices costs money. Already limited IT resources will need to be taxed further to support them and new skills will be needed to maintain these devices on an ongoing basis. In some cases, the company may need to invest in third-party management software, adding to the cost of support. That said, consumerisation can also be a cost killer when the procurement and management of devices is off-loaded to the user.

- **Security**: New devices and social applications are bringing potential security risks to the enterprise and public sector organisations. These risks are varied and can take the form of data leaks and viruses on the devices as well as lost and stolen devices that contain corporate and private information. Do businesses and organisations understand the issues, and do employees fully understand the risks?

- **Compliance**: If organisations allow personal devices to hold corporate data, who is responsible for the security and privacy of that data? What about the personal information on the device that is private to the individual? These issues mean that the pressure brought about by consumerisation needs to be addressed from a legal perspective. Compliance auditing will also be important to ensure unmanaged devices are compliant with corporate policies and do not pose a compliance risk.

- **Brand**: Consumerisation allows for almost instant collaboration, information sharing, and flexibility within the extended enterprise, but when it goes wrong, it does so with a click of a mouse and can significantly damage the corporate brand.

- **Culture**: What will the cultural impact be if IT departments allow some employees specific devices of their choice on the network (e.g., the iPad) but blacklist other employees from doing the same? If the CEO sets an example, should the remaining employees expect less?

Managing the Risks of Consumerisation

At the heart of the ubiquity of mobile access to IT resources, especially for network-enabled applications, is the consumerisation of IT. There are two contrasting IT philosophies when it comes to addressing the consumerisation of IT. One is to lock everything down and not allow any new or unauthorised devices on the network and to block all access to social or Web 2.0 apps in the workplace. The basis of this philosophy is that the risks and complexities are too great and best practices are not yet defined, therefore controlling everything overrides employee preferences or, indeed, potential productivity benefits.

The second philosophy is to fully embrace the concept, allow information to flow liberally across the organisation as part of the normal IT procedure, and only block certain devices, practices or applications that are deemed unnecessarily peripheral or too risky.

Unfortunately, whichever way you look at it, there are no perfect answers and much depends on the specific culture and industry sector. That said, IDC can provide five important IT criteria to consider when addressing consumerisation:

- **Assess the risk**. The first step is to acknowledge that there are risks associated with consumerisation. Can existing security policies be maintained, or do they need to be adapted based on business needs?

- **Set clear policies based on functional profiling**. The next step should be a series of specific policy decisions based on functional profiling of employees to determine who realistically needs access to what in terms of devices and applications. The criteria for these decisions are often business and public sector organisation-specific and industry-specific. In

most cases, however, blanket policies from the CEO down to all employee levels tend to be difficult to enforce.

- **Acknowledge that policy needs to be dynamic**. What works today may not necessarily be best in three months. Policy frameworks need to be adaptive, dynamic and responsive to many changing elements within organisations, whether technological, policy-based or cultural.
- **Develop contingency plans**. IT should ask the question: "What would we do if…?" and think through the all the risk scenarios that consumerisation brings.
- **Training and communication**. IT should also communicate effectively with all employees, so that they are aware of and accept not only the security policies of the organisation, but also of their moral and behavioural responsibilities and the consequences of malpractice.

What Should Organisations do to Leverage Safe and Compliant Use of Mobile Devices and Allow for Mobile Ubiquity?

1 ─ Get a Full View of Risk and Threats

IDC believes that one of the key challenges is to determine the ownership of data on a mobile device. Some personal data can be hosted on a company owned device, some company data can reside on a personal device. A mapping of data suitability per device is a must-do before any further action is taken. A specific policy should be implemented for this complex pairing.

More generally, distant, remote and mobile connections expose users, devices, data and infrastructure to the global risk of the connected world:

- Internal IT weaknesses create vulnerabilities (almost 5,000 new vulnerabilities discovered each year)
- Attacks by hackers, bots or ghost networks in search of value (money, data, credentials), or for military or political action
- Common threat exposure such as viruses (even though there a lot fewer viruses for mobiles), spam, malware
- Network-based attacks ("man in the middle", intrusion)

The risks associated with ubiquitous mobility cannot be seen as simply a replication of the current threat of the connected world. Very few viruses are officially disclosed and the list isn't growing. There is not enough energy or computing resources available on a mobile device for traditional viruses to exploit. In short, not much can be done from a mobile where most of the energy is directed to the screen and its millions of colours. As a result, protecting mobile devices from viruses and spam doesn't seem to be an urgent technical priority for most IT organisations. However, there are risks posed by mobile devices connecting to the Internet and messaging systems, most notably:

- **Mobile data**: Mobile devices can store a few dozen Gigabytes of data on a local disk or storage disk. This data can be critical for organisations and should be protected by an effective and managed encryption strategy. Advanced DLP solutions can monitor what data is transferred to a mobile device, smartphone, or mobile storage device.
- **Mobile identity credentials**: Many smartphones carry identity credentials to be used during authentication. Those credentials must be protected in case of device theft so that identity theft or abuses can be prevented.
- **Mobile browsing**: Mobile browsing should comply with an organisation's Internet browsing policy. A local (or gateway-based) control must apply to prevent regulation or policy breaches, rogue browsing and visiting high-risk Web sites.
- **Mobile phone call logs and details**: Mobile devices are very often phones. Some basic functions such as calendar, directories, and call logs can be accessed and thus breach business confidentiality. Therefore, phone details must also be stored and protected to

prevent unauthorised access to confidential information. In the case of the use of *personal* mobile devices to store and transfer data, their necessity should be assessed and approved by the IT department, at which point it is essential to ensure compliance and that usage conforms to corporate policy. If it is deemed essential to use personal mobile phones in this way, the security policy should be strictly applied.

2 — Compliance Also Applies to Mobile Tools

Current regulations in Europe that apply to IT apply to endpoints of any kind (mobile or otherwise). Mobile tools are not an exception. The main regulations are:

- Privacy ─ Directive 136 & 140, The European Privacy Framework
- Credit card payment security ─ PCI-DSS
- Anti-terror and national security
- Digital rights and anti-piracy for media and intellectual property owners acts

In a regulated environment, user activity may need to be monitored, logged and in some cases kept for legal evidence or clearance purposes.

Whenever organisations consider compliance processes, they should include mobile tools as part of the initiative, applying the same processes for smartphones as for any fixed-line device.

Technology Considerations: Cisco AnyConnect Secure Mobility Solution

Cisco has launched many products to help address customers' challenge of enhancing productivity without compromising network security. Cisco's AnyConnect Secure Mobility Client enables desktop and mobile users to connect to Cisco's Borderless Network, giving access to the network from inside or outside the firewall from any device based on comprehensive secure access policy. The AnyConnect Secure Mobility Client has been designed to work in conjunction with Cisco's IronPort Web security appliance, the Cisco ASA appliance, and also provides integration with ScanSafe, which is an in-the-cloud Web security solution.

Cisco's approach to bringing security to the top of its priorities is the right one. Traditional security controls have been primarily network-centric (ACLs and firewalls) and host-centric (file system permissions). And even though these controls are important to protect borderless networks and cloud environments, they are not enough to stop malicious attacks to the network, because the boundaries set within a premises-based network are not as strongly defined when mobility, consumerisation of IT and Web 2.0 applications are introduced into the environment.

Bringing to market new security functionality specific to borderless network and cloud environments is a clear step toward addressing customers' needs to manage risks posed by mobility and demand for increased flexibility, built into the network policy and access controls for an automatic, context-aware and adaptive network security solution. Cisco's AnyConnect Secure Mobility Solution is well positioned to address this need.

Key Challenges: Securing the Mobile Worker

- Fight proliferation… but do not kill productivity! The worst thing to do is prevent employees and partners from connecting mobile tools. The adoption of tablets and smartphones is increasing and the business drivers are sufficient that the trend will not slow down for security considerations. Ease of use, portability and ubiquity have many positive benefits for users, so it is advised to help users leverage them in a secure and compliant environment rather than force them to adopt constraining security policies.
- Since organisations experience real business advantages in allowing smartphones to proliferate, security experts must find a way to support these productivity benefits while at the same time managing the chaos they create. The goal should be to provide tailored, agile, smart and effective security and compliance solutions for mobile, distant, and remote users rather than apply rigid policies that are difficult to enforce and unlikely to meet the diversity of

needs of business users in an organisation. Let the BYOC (bring your own computer) phenomenon happen.

- BYOC or consumerisation can relieve some of the costs of supporting and maintaining endpoints. It also gives the user responsibility for device choice and handling. While BYOC forces central IT organisations to accept a locked part of a non-owned device, there are security and management solutions designed to help manage BYOC. These solutions can help organisations to both leverage the benefits that proliferation provides and help manage them with robust and compliant management tools.

Global Headquarters: 5 Speen Street Framingham, MA 01701 USA P.508.872.8200 F.508.935.4015 financial-insights.com