

THE CONSUMERIZATION OF ENTERPRISE MOBILITY: Yes, a Formidable Challenge, but also a Great Opportunity

As more and more consumers invest in smartphones, tablets, and other web-enabled mobile devices, enterprises of all sizes are being confronted and challenged by employees who want to use these same devices for full access to their professional lives, in addition to their personal ones. This trend, the "consumerization" of enterprise mobility, represents a formidable challenge as well as a great opportunity for organizations.



When coupled with the growing availability of high-speed Wi-Fi, cloud-based services, and virtual technologies, these mobile devices can easily support a flexible business environment, fostering the ability for working anytime, anywhere. The distinction between business and leisure time is no longer dictated by a traditional 8-to-5 schedule. On a personal device, employees can transition between business and personal tasks seamlessly, allowing them to work when they're most motivated.

Consumerization offers organizations great potential for increasing individual productivity and reducing overall information technology costs. However, it also creates security risks, potential financial exposure, and increased operational headaches for organizations. It is a dilemma that is keeping many business managers and IT professionals awake at night.

Survey by **VansonBourne**:

78 percent of CIOs don't know what devices are connected to the corporate network, and 77 percent of enterprises don't know what data is lurking on all of those devices. Only one in three can track these devices, and only half of all those surveyed said they could secure these devices should they be lost or stolen. Three-quarters of those surveyed said that "security headaches" are actually caused by the mobile devices.



Organizations Need to Embrace Employee Mobile Devices

Despite the loss of sleep because of consumerization concerns, IT decision makers need to accept the trend as an unavoidable transformation. They must embrace consumerization in order to leverage the benefits that come with what some are calling a revolution as big as the advent of the PC. The risk of fighting against consumerization is that a business will waste time and money and, ultimately, be surpassed by competitors who are more flexible, progressive, and ahead of the curve.

Keeping the consumer-type technologies out of the workplace simply isn't feasible any longer. The sheer number of devices in employee hands, many of which include their own access to the Internet, makes policing the situation nearly impossible. Clearly, in today's economy where IT departments are being asked to do more with less, this is a waste of valuable resources.

Therefore, any smart organization is going to harness the power inherent in consumerization and exploit its obvious benefits while trying to manage its potential hazards. In order to do this, IT leaders and staff members will have to resolve three major issues:

1. How to support devices that they didn't purchase and may not know are on their network
2. How to secure the corporate networks and business data accessed by employee-owned smartphones and tablets
3. How to differentiate corporate content from personal data on employee-owned devices that are accessing the network

Meeting the Challenges for Enterprises

By embracing the consumerization of IT, organizations can keep the employees happy, save money, and provide their IT department with some hope of keeping track of what devices are being used and how.

Many organizations are approaching the consumerization challenges with a three-tiered approach* that is based on the function and business role of the employee

requesting access and their desired device's platform. The three levels of access for devices are linked to the extent to which they are managed by the organization's IT operations:

- **Unmanaged devices** - Employee-owned devices with baseline security, granted access to web-based email but no business apps. Sometimes called "bring your own device," or BYOD, this approach is the least favored by IT organizations, especially outside the United States.
- **Lightly-managed devices** - Employee-owned devices subject to security and management requirements, including installation of Security and/or MDM agents and enforcement of policy requirements, these devices are usually Android™, iOS, or Windows®-based and have access to corporate email, calendaring and intranet, but limited business app access, and will continue to run many personal apps.
- **Fully-managed devices** - Corporate-owned devices with full security and MDM capabilities and supported by corporate IT and Helpdesk, these are usually BlackBerry® and sometimes iPhone®, and have complete access to corporate messaging, calendaring, and business applications, and some or no personal apps installed.

Of these approaches, the Lightly-Managed and Fully-Managed levels of access provide use cases for products such as **Trend Micro™ Mobile Security 7**, which is a comprehensive mobile device security management solution. It bridges the gap between mobile device management and traditional endpoint security solutions.

By combining cloud-based security enforcement and mobile device management capabilities, Trend Micro Mobile Security 7 lets organizations securely embrace consumerization. It also supports the increased mobility of enterprise workforces, without exposing users and data to risk.

*= Benjamin Gray & Christian Kane, "Mobile Device Strategies for Supporting Consumerization," Forrester Research Group, May 2011.



The **Trend Micro Mobile Security 7** combination of **security and management** features enable enterprises to:

- 1.** Manage mobile devices to minimize cost
- 2.** Ensure devices are safe to access the corporate network
- 3.** Secure the data on missing devices

The Results - "Bring 'Em On!"

Trend Micro Mobile Security protects devices, data, and corporate infrastructure; lowers the cost of supporting mobile users and the devices of their choice; and alleviates IT burden by providing visibility and control. The results are:

- Fewer data loss incidents - Preventing data loss by enforcing a restrictive access policy to devices limits the risk of data loss incidents. And the ability to remotely wipe all content from a lost/stolen device not only protects the data on the device, it also helps meeting compliance requirements and may prevent having to report a data breach, which could have a much more far-reaching impact on the reputation of the organization.
- Decreased security risk - Ensuring the proper device configurations and adding protections to prevent malware reduces the risk of compromised devices. It also facilitates complying with regulations.
- Reduced operational costs - Facilitating user access to resources saves significant IT resources, as provisioning configurations over the air rather than on the device itself frees IT support time. Built-in support capabilities further reduce the IT support effort required to enable and maintain user productivity with mobile devices. Built-in usage tracking and reporting capabilities unlock hidden savings by making optimization potential in network and voice communication visible.

With Trend Micro Mobile Security 7.0, enterprises can aggressively embrace consumerization and their IT departments can confidently say to employees with their own devices, "Bring 'em on!"

You can be sure that over the next year many more security and management solutions will be rolled out to help companies handle the consumerization of enterprise mobility. It's really up to you: either meet the challenge and take advantage of this opportunity; or close the doors and be left behind.

Survey by **CSI**:

According to a CSI Computer Crime and Security Survey, 7% of total financial losses incurred by businesses from IT security incidents were related to the loss of proprietary or confidential data resulting from mobile device theft.