TREND MICRO

Trend Micro
Enterprise Security

"*Bring 'em on!*" –
The Consumerization
of Enterprise Mobility

A Trend Micro White Paper | July 2011

I. WHAT IS "CONSUMERIZATION"?

"Consumerization" is the name for the trend where employees use their own devices and consumer applications to conduct company business. These devices include smartphones, pads, and tablets with their own external data plans. Consumerization is having an enormous impact on how enterprise IT departments protect endpoints and secure corporate data.

This movement is quickly transforming the way employees and companies work. Although not every enterprise IT manager refers to this growing trend as consumerization, most have been confronted by aspects of it. The implications of the widespread use of personal devices in the workplace are forcing changes to the philosophies and practices of IT professionals.

Many workers today have access to powerful computer systems and high-speed Internet at home. So as technology grows increasingly important in their personal lives, employees have become accustomed to the power and convenience of consumer Web 2.0 applications, along with the flexibility of data exchange with cloud-based storage, webmail, and ubiquitous Internet connectivity.

With the surge of powerful personal mobile devices, a significant shift in the landscape of client computing devices and the accessing of corporate data is occurring. The company-provided Windows® laptop is no longer the only option to employees. Now, staff members are reading email – both private and business – on smartphones and mobile devices that can access the corporate CRM on tablets, and store corporate data on their non-PC laptops, or netbooks.

> In a September 2010 Computerworld survey, 75% of all organizations claim to already support the use of employee-owned mobile devices. [1]

Consumerization has turned many offices into environments where employees can BYOD.

II.   WHAT IS BYOD?

The first sign of enterprises embracing the consumerization of their IT begins with "Bring-Your-Own-Device" programs. BYOD programs indicate that enterprises not only tolerate the use of personally-owned and user-liable devices, but actually encourage and sponsor it.

When employees choose their own devices, and enterprises provide an allowance or sponsorship for those devices, the result is a win-win scenario. The employees get devices that they are allowed to use for private purposes, and corporate IT shares off-loads some or all of the cost of the hardware and data plan to the employee. Moreover, employees are happy because they get to use the devices of their choice, in a flexible, work-anywhere manner, and the employer is happy to capture the increased productivity and employee satisfaction that come with it.

The trend of BYOD is supported by other trends, such as smartphones outselling traditional PC devices [2]; Generation X worker who require and expect anytime, anywhere access to information; and the large numbers of consumers who expect to be using their private smartphone for work. (See stats and graphics below.)
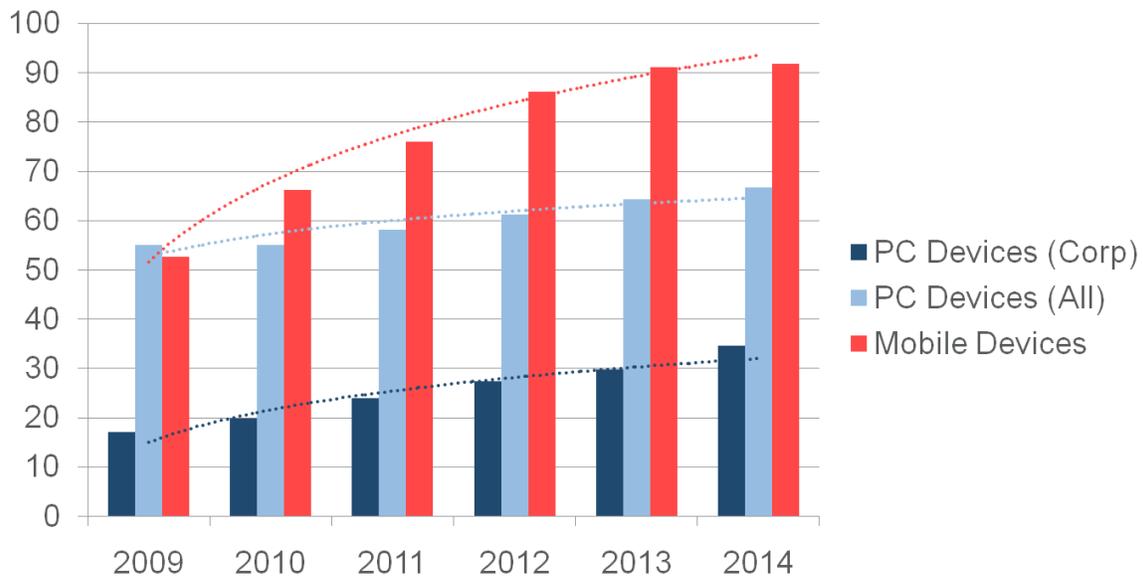

Figure 1: IDC reports Smartphones outsell PCs for the first time in 2010

In a recent survey conducted by Trend Micro, 45% of the surveyed consumers expect to be using their private smartphone for professional work.
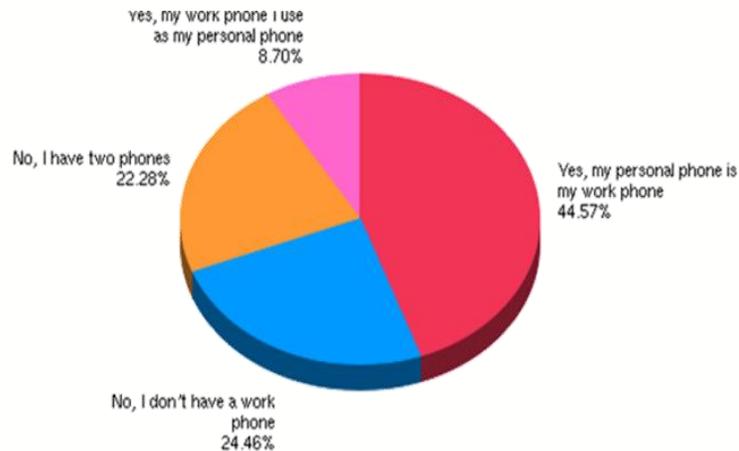

Figure 2: Personal Phone Used for Work Survey

III.   HOW CAN YOUR COMPANY BENEFIT FROM CONSUMERIZATION?

The business benefits of extending enterprise data and applications to mobile workers are already apparent:

- Consumerization enables remote workers to be more productive
- Leads to higher customer satisfaction
- Leads to the higher retention rates of talented employees
- Can cut IT costs on operations, hardware, and software licensing

Recent studies indicate that almost half of the U.S. workforce is already mobile and away from the primary work location for more than 20% of the time. [3] In fact, in a recent NetworkWorld.com article, Jenny Englert, a Xerox senior cognitive engineer, in a study "found that mobile workers were outside the office about 80% of their workday."[4] Mobile workers may include road warriors, field workers, day extenders (checking email from home before going to the office), business travelers, teleworkers, and other engines of the knowledge-based economy.

It is probably fair to say that most corporate employees are already occasional mobile workers, as the traditional boundaries of the office have blurred into homes, hotels, conference centers, airports, busses, trains, airplanes and many other commercial venues such as coffee shops and malls.

Increasingly, a company's ability to compete depends on enabling mobile workers to be productive wherever they are and respond to market demands in a timely manner. In fact, according to a Yankee Group survey, workers say that "working from home is the single most important improvement their organization can make to improve their productivity." [5]

Consumerization also has the potential to save time and money on both, operations, hardware, and software license costs. According to CIO magazine, Avago, a semiconductor company that moved its employees over to Google Apps, has saved $1.6 million a year. In the United Kingdom, not long after implementing Gmail and dropping Exchange, the construction firm Taylor Woodrow claims to have saved $2 million. [6]

IV. HOW CAN THE IT DEPARTMENT MANAGE AND SECURE EMPLOYEE MOBILE DEVICES?

IT departments in consumerized environments are faced with a series of challenges, mainly around acquiring visibility and some level of control over the plethora of user-liable devices.

- Management of user-liable devices

Management in this case has a dual purpose. First, it is about making the experience for the user a smooth and easy one, in order to maximize his motivation and productivity. Second, it's getting some level of control over user-liable devices to minimize the exposure to security risk. A well-managed device is – in most cases – a safer device.

- Exposure of sensitive corporate data stored on devices

There are several ways for sensitive corporate data to be exposed to unauthorized third parties. Millions of cell phones and laptops are lost or stolen every year. Sensitive data stored on the device must be considered compromised, and depending on the nature of that data, a data breach must be reported to the authorities, resulting in cost of up to $50,000 per exposed device and a loss of reputation.

- Leakage of sensitive corporate data through consumer applications

As employees use the same device for personal and work-related tasks, sensitive data can easily – with or without malicious intention on the side of the user – be transferred off the device. It can be sent via Webmail, instant messaging or other non-corporate communication channel.

- Introduction of malicious data or software

Malware can be brought into the corporate network in multiple ways. A user-liable device can get infected by simply surfing the web under-protected or by being used in an insecure environment.

Trend Micro, a global cloud security leader for 20+ years, can help. Trend Micro creates a world safe for exchanging digital information with its Internet content security and threat management solutions for businesses and consumers. As a pioneer in server security, we deliver top-ranked client, server, and cloud-based security that meets our customers' and partners' needs, stops new threats faster, and protects data in physical, virtualized, and cloud environments.

Powered by the Trend Micro™ Smart Protection Network™ infrastructure, our industry-leading cloud-computing security technology, products, and services stop threats where they emerge, on the Internet, and are supported by 1,000+ threat intelligence experts around the globe.

The Smart Protection Network delivers security that's smarter than conventional approaches by blocking the latest threats before they reach you. Leveraging cloud computing across Trend Micro's security solutions and services, the Smart Protection Network provides a stronger cloud architecture that protects your computer network and corporate data while reducing your reliance on time-consuming signature downloads.

Trend Micro's expertise in securing corporate environments helps you confidently handle the challenges of consumerization of enterprise mobility.

V.   ENTERPRISE AUTHORITY VS. EMPLOYEE PRIVACY

There's a potential bump in the road to consumerization that many may not have considered. It stands to reason that when an employee brings their personal device into play with professional work, that there is a large potential for conflict. The conflict arises when an enterprise's IT department's need to have enough control over the mobile devices that are accessing corporate networks to keep them secure and yet also meets the employee desire to keep the personal data on their personal devices private.

In two different recent Trend Micro surveys, we see the interests of the two constituencies arising and potentially blocking each other in the consumerization trend. When asked by Trend Micro, a vast majority (91%) of company employees said they would not grant their employer control over their personal device in order to access corporate applications. Then when surveyed, nearly 80% of enterprises stated that they would require to "have the authorization or control to enforce installation of management mechanisms on the mobile devices." We also found in other instances that an overwhelming number of IT managers believe that companies should be able wipe personal (in fact all) devices that connect to corporate networks.

Clearly, employees feel strongly that they should be able to protect their personal data from company invasion while IT professionals feel they need complete control of any device that is used to interact with the enterprise's machines and data. So what's the best way to manage the concerns of both parties?

In a recent report, Trend Micro's Cesare Galati recommends taking "a thoughtful, strategic approach to consumerization and develop a cross-organizational plan. IT cannot do this in a vacuum and should certainly engage executives, line of business owners (marketing, sales, HR, product development) as well as customers, partners, and internal early adopters."

"While planning to adopt new consumer technology, IT managers should survey their most innovative users to discover what devices and applications they prefer and what they find most useful in their work activities. This way, IT can effectively pull from users' experience, rather than pushing IT views to their base."

"The second step is to develop a firm set of policies that clearly define what devices and applications are considered corporate standard (fully supported by IT) vs. tolerated (jointly supported with the user) vs. unsupported (full user liability). In addition, IT will profile the global workforce based on relevant attributes such as role, line of business and location. IT will then map technologies to user profiles and define SLAs for each intersection."

"The third step is to deploy appropriate IT tools specifically designed to secure and manage consumer technology in the enterprise. While some solutions have already materialized along the lines of specific product segments, no single vendor can provide one single solution covering all functional requirements across all platforms."[7]

VI. CONCLUSION

The consumerization and mobilization of enterprise IT is a real, irreversible, and unstoppable movement that needs immediate attention and innovative solutions. In order to maintain secure endpoints, as the potential for breach expands, IT departments must be flexible and inclusive when developing polices so employees are encouraged to use their personal mobile devices without fear of losing control over them.

When guided and supported by the proper tools and policies the consumerization benefits can be huge for all involved parties in that:

• Employees are now able to choose and work with the devices of their own choosing, where and when they are most productive

• IT is unburdened from device support, helped with regulatory compliance and can focus on more strategic security goals

• The management gets more satisfied and productive employees and an advantage over competitors who are still trying to figure out how to contain the unstoppable

Trend Micro provides solutions to address numerous critical challenges in consumerized and mobilized enterprise environments, enabling enterprises to securely embrace and unlock the benefits of the consumerization of their IT.

FOR MORE INFORMATION: http://us.trendmicro.com/us/products/enterprise/mobile-security/

VII.   RESOURCES

[1] ComputerWorld survey
http://www.pcworld.com/businesscenter/article/210079/getting_it_set_for_mobile.html

[2] IDC Worldwide Quarterly Mobile Phone Tracker, January 2011 and IDC Worldwide Quarterly PC tracker, January 2011

[3] Yankee Group Study, "Maximizing Mobile Worker Productivity," 2008

[4] NetworkWorld.com article
http://m.networkworld.com/news/2011/062711-desktop-doomed.html#mobify-bookmark

[5] Yankee Group, 2008 Blended Lifestyle Survey—U.S. Large Enterprise

[6] CIO Magazine: "Why Enterprises Are Moving to Google Apps, Gmail", June 10, 2009

[7] "Why You Should Embrace Consumerization: Learn the steps to managing your workforce without limits" a report by Cesare Garlati, Sr. Director Consumerization & Mobile Security, Trend Micro
http://us.trendmicro.com/imperia/md/content/us/pdf/solutions/enterprisebusiness/virtualdesktopsecurity/tlp01_consumerization_thought_leadership_110617us.pdf