Mobile Consumerization Trends & Perceptions

IT Executive and CEO Survey

FINAL REPORT

COMPARISONS: WAVES 1 AND 2

PREPARED FOR:

TREND MICRO, INC.

BY:

DECISIVE ANALYTICS, LLC

Cheryl Harris, Ph.D.
Chief Research Officer
Decisive Analytics, LLC

575 Madison Ave, 10th Floor
New York, NY 10022

917.628.6167

August 2012

EXECUTIVE SUMMARY

Overview and Objectives

The overall objective of this project is to assess awareness of issues related to IT/computing consumerization within the enterprise, and to learn about**:**

- **Attitudes**
- **Perceptions**
- **Internal policy development related to consumerization**
- **Other emerging concerns**

"Consumer IT" has been identified as a significant cross-industry trend, with an enterprise survey (DELL/KACE, *CIO Magazine*, Sept. 15, 2011) demonstrating that 87% of executives say their employees are using personal devices for work-related purposes, with tasks ranging from email to calendaring, to ERP and CRM functions. This has placed pressure on management to develop effective policies surrounding the incorporation of personal devices, cloud services, and other manifestations of "consumer IT" in the workplace.

In order to better understand how this is affecting the workplace IT environment and how executives are making sense of it, the study targeted management with direct and recent involvement in considering the impact of consumerization at their company and/or making policy decisions related to it.

Methodology

An online survey was conducted with IT executives and CEOs of larger companies (500 employees or more) located in the United States, United Kingdom, and Germany. The first wave of interviews was conducted between January 3, 2012 and January 11, 2012, and the second survey was conducted between April 10, 2012 and April 20, 2012. The second wave of interviews was conducted with a new sample that had not participated in the first wave. Most of the initial survey questions were retained for the second wave, along with a few selected new questions.

Waves Compared by Surveyed Groups

	Wave 1 N=	*Wave 2 N=*
CEO	**26**	**21**
IT Senior Executive	**410**	**415**
Total	**436**	**436**

Wave1 *(January 2012)*
436 senior executives were interviewed in total. 410 interviews were conducted with IT executives (50% U.S., 25% U.K., and 25% Germany). An additional 26 interviews included only CEOs of larger companies across the same three countries.

Wave 2 *(April 2012)*
436 senior executives were interviewed in total. 415 interviews were conducted with IT executives (50% U.S., 25% U.K., and 25% Germany). An additional 21 interviews included only CEOs of larger companies across the same three countries.

Profile: Combined Waves

Respondents included employees of companies ranging from a minimum of 500 employees to more than 20,000 employees in the U.S., U.K., and Germany. The primary business activity of the companies at which they were employed included accounting, business services, engineering, government, transportation and utilities, with about 15.5% overall saying they were in manufacturing, while another 15.9% described the company focus as IT consulting or system integration.

825 respondents were senior IT administrators, and 47 were the CEO of their company. The most common IT titles were IT manager/administrator (30.6%), CIO/CSO/CTO (20.9%) and VP/director of IS/IT security (20.3%).

Respondents were required to have at least some influence on decisions regarding the devices their company's employees could or could not use to access the company network. Most IT executives (62.3%) said they were primarily responsible for such decisions. Not surprisingly, nearly all (93.6%) of CEOs said they were the principal decision makers.

BYOD Practices & Drivers

Nearly all companies (76.7%) in this study allow employees to use their personal devices such as laptops, netbooks, smartphones, and tablets for work-related activities.

U.S. executives were more likely to say their company permitted BYOD (80%), compared to executives in the U.K. (70.8%) and Germany (75.4%). Interestingly, executives under the age of 45 were more likely to say their companies permitted employees to use their own devices at work.

Virtually all companies surveyed apply an IT security policy to employee owned devices that access the company network (89.7%), and also require that devices either be on a pre-approved list and/or pre-approved with security software installed (53.7%). They also plan to segregate corporate applications and/or data when personal devices are used for work purposes (71.2%). Additionally, more than 80% require employees to install security software on personal devices.

CEOs are enthusiastic users of multiple mobile devices, with 84.8% saying they use smartphones at work, while 73.7% of IT executives said they do the same. The second most frequently mentioned device was a laptop (CEOs 78%, IT execs 68%), followed by an iPad or tablet (CEOs 82.6%, IT execs 45.2%). About a third said they use mobile software or apps, and about the same said they use online data storage or cloud solutions. Nearly the same proportion reported using Facebook (32.4%), LinkedIn (20.4%), Twitter (18.8%) or Youtube (13.1%). CEOs, though, were more than twice as more likely to say they use YouTube compared to IT executives.

There are multiple operating environments associated with consumer mobile devices, and many companies restrict those that will be permitted for use on the company network. Most common among permitted devices are Android (69.3%), and Blackberry (69.2%), followed by iOS (53.6%), Windows (50%), and Symbian (24%).

Asked to rank the above mentioned operating systems for their security and manageability, Blackberry fared best, followed by iOS in second place, with Android close behind. Windows came in fourth followed by Symbian in last place.

Very few companies said that all devices in use company-wide are owned by employees but estimated that a third or less than a third of devices in use are employee owned. Laptops, tablets, netbooks, portable storage, and mobile software/apps are more often owned by the company than by the employee.

However, smartphones are more commonly owned by the employee, by a slight margin.

Nearly 80% of companies have implemented Virtual Desktop Infrastructure (VDI), in client hosted or remote synchronization mode. Just 15% had not yet deployed VDI.

The OS used by the company on non-mobile computing devices (servers/desktop) is overwhelmingly Windows (77.7%), although some use Mac OS as a primary OS (13.5%), and others said they use Linux (7.6%) or Unix Based (1%).

The **top drivers** executives mention behind employee-owned device use at their companies are:

- Improved mobility (ability to work offsite or on the go (43.1%)
- Avoidance of carrying or maintaining multiple devices (13.6%)
- The view that BYOD is an employee benefit (10.5%)

Security Breach Experience

Nearly half of companies that permit BYOD reported experiencing a data or security breach as a result of an employee-owned device accessing the corporate network (46.5%).

Responses to security breach events related to employee-owned devices varies, but the most common response is to restrict data access rights (45%), and require immediate installation of security software (42.9%) or simply to revoke BYOD privileges (11.6%). German companies are slightly more likely to insist on security software installation in response to a breach, while U.S. companies are somewhat more likely to shut down BYOD access.

Companies did say that they have a policy of remotely wiping a mobile device both when it is lost and upon employee separation (35.5%), while some do so only in the case of a lost device (23.3%). A few said they selectively wipe corporate data applications when necessary (10.1%).

Security Software

Most companies (83%) require employees to install software to secure and manage their personal devices when used for work purposes. We asked the companies that do *not* require security software why they did not require it. Surprisingly, the most common responses were: “We only allow trusted users to connect to the network,” (25.7%); and, “We are not concerned about security on these devices,” (15.6%).

Some say they have not had a security software solution (13.8%) or are still researching a security solution (12.8%). User rejection (11%), perceived high cost (10%), and perceived complexity (3.7%) were less frequently mentioned.

Considering smartphone security alone, nearly all (89.5%) expressed concern about data security on smartphones.

Acceptable Use Policies (AUP)

Most companies (79.7%) indicated they had released an acceptable use policy (AUP) to employees related to company/employee responsibilities with respect to employee-owned device use, security, and liability.

Asked which of several components companies included in their AUP documents:

- 12.2% state that in case of device loss, devices could be remotely wiped by the company.
- About 10% include statements to the effect that corporate IT will routinely monitor data, downloads and other activity on the mobile device, and/or in cases of corporate litigation, data on the device could be subject to exposure, or the device itself could be seized.
- 9.7% state that incorrect login attempts could result in data deletion, that geographic location of the device may be tracked, or that the company has liability for data on the device.

BYOD Impact on Costs

The introduction of employee-owned devices may impact costs associated with supporting BYOD, with some companies finding that overall costs may either increase or actually decrease with the advent of BYOD, and for many reasons.

Interestingly, nearly 40% of companies said that **costs decreased** after introducing BYOD (39.3%). Combined with those who said that costs remained the same (23.3%), a majority of companies agreed that BYOD had either decreased costs overall or had no cost impact.

Interestingly, respondents in the second wave (April 2012) were less likely to report that BYOD had increased their costs overall, and significantly more likely to say that costs had either remained stable or decreased, than respondents to the first survey in January 2012. It may be that cost impact assessments improved with

more BYOD experience or that overall costs associated with BYOD simply became lower in the successive months.

Reasons that costs were seen to decrease were split nearly equally between lower IT capital expenditures, mostly due to employees purchasing their own devices (37.9%), lower desktop tech support costs (31.3%), and higher employee productivity (29.6%).

Among those that said that costs have increased as a result of BYOD, the primary reason cited was increased tech support costs (41.2%) or increased capital expenditures for VDI (31.5%). Higher software or software virtualization costs were less frequently (27%) cited.

Asked directly about the overall impact of employee-owned devices in the company, it becomes clearer that BYOD both introduces some transitional costs as well as benefits that may outweigh those costs, such as increased employee productivity, satisfaction, and customer satisfaction.

Additional Impact of BYOD

The real impact of BYOD, then, may well be on the corporate culture and organizational philosophy. Several interesting findings emerged when we asked senior executives how much they agree or disagree with statements describing the impact of BYOD.

Executives agreed that permitting BYOD provides a competitive advantage, is an employee benefit, is useful to recruitment/retention, and that employees have “a right to use their own computing devices for work.” Employee use of their own devices is seen as significantly boosting creativity and innovation, and improving work-life balance.

CEOs were more positive about the impact of BYOD than were IT executives. Interestingly, there is a gap between the CEO perspective and the extent to which IT executives thought their company would view each statement, suggesting that IT executives may not be as tuned in to the views of the CEO as one would expect.

The majority of respondents (62.9%) agreed that permitting employee-owned devices at work positively influences the employee's view of the company, and nearly half (47.5%) said that it positively influences the customers’ view of the company.

The Future of BYOD

Growth of BYOD is widely seen as inevitable in the companies we interviewed. In fact, many thought it would be more prevalent for all company users in the future. About a fifth thought it would replace PCs for a majority of users (17%) although some said it would be used primarily for communication and messaging tasks (14.7%).

Companies are actively planning how they will continue to incorporate BYOD in their organizations. Among the changes in consideration are acquiring new software or technology to manage security issues (21.4%), reorganizing the IT department (20.3% -- but notably more popular among CEOs, with two-thirds saying they would favor reorganizing the IT department), moving to a thin architecture platform or redefining how computing devices in general are supported (14.6% and 16.2%, respectively).

More than a quarter predicted they would reallocate budgets away from purchasing computing devices and a few would reallocate software budgets (8%).

We also asked all respondents to briefly summarize their views on what challenges they see ahead for BYOD in their companies. While a few respondents flatly rejected BYOD as impractical in their own industry and/or company (such as Government staffers) **most said "BYOD is the future."**

CONCLUSIONS

1. **BYOD is already common**, with more than three-quarters (76.7%) saying that employees are permitted to use their personal devices such as laptops, smartphones, and tablets for work. This is more commonly the case for U.S. firms than for companies in the U.K. or Germany.

2. **Nearly all companies that do permit BYOD require security software** to be installed on personal devices. A variety of vendors are servicing this software market. Reasons not to install security software varied, but there is almost universal concern about smartphone data security (85.9%).

3. **Security breaches have been experienced by nearly half of all companies** that allow BYOD and immediate changes to security protocols typically follows such breaches, with data access right restrictions (45%) or security software installation (42.9%) being the most frequent responses. Few shut down BYOD altogether following a breach.

4. **CEOs are generally more enthusiastic about BYOD than are IT executives,** the latter being all too aware of the security challenges and support issues that BYOD presents. CEOs use multiple mobile devices themselves and are likely to say it enhances their own productivity as well as that of employees.

5. **BYOD gives companies a competitive advantage.** Nearly half of CEOs said that BYOD offers a competitive advantage, while slightly fewer IT executives said it does not.

6. **BYOD is seen as an employee retention and recruitment tool.** Almost half of CEOs (46%) and IT executives (42.5%) agreed that BYOD is an employee benefit and used to attract or retain employees.

7. **BYOD enhances innovation and creativity, boosts productivity.** BYOD is seen to improve employee productivity (47% of CEOs agreed, 46% of IT execs), as well as innovation and creativity (50.7% of CEOs, 48% of IT execs).

8. **Employees prefer companies that permit BYOD, as do customers.** The majority of respondents (62.9%) agreed that permitting employee owned devices at work positively influences the employee's view of the company, and nearly half (47.5%) said that it also positively influences the customers' view of the company.

9. **BYOD *decreases* or does not impact overall costs.** While BYOD necessitates expenditure on security software and support, insisted upon by most companies that allow it, the impact of BYOD is a decrease in overall costs or no net change. This is an important finding that should be shared with companies interested in introducing employee-owned device policies, since more than half of those surveyed said that costs either decreased (36%) or remained the same (20.1%).

10. **Is BYOD an employee right?** Nearly half of CEOs thought so. This is a provocative question and one deserving further investigation.

11. **Acceptable Use Policies (AUP) are in place at nearly all companies** permitting BYOD. When asked about the components of the AUP documents, the ability of corporate IT to remotely wipe devices is the most common provision, followed by the right to monitor activity, the possibility that data may be exposed in case of litigation, and that incorrect login attempts can cause data deletion.

12. **BYOD growth in the workplace is seen as inevitable.** However, senior management is clear about the possible risks and ready to invest as needed to make deployments as smooth as possible.