WHITE PAPER

Managing PCs and Devices in Changing Technology Times

Sponsored by: HP

Robert Young   Raymond Boggs
Tim Grieser
June 2013

EXECUTIVE SUMMARY

As companies grow beyond their small business roots to become midsize or larger, the management of PCs and other end-user technology such as smartphones and tablets becomes an ever greater challenge. Simply keeping track of devices is just the starting point. Firms also need to manage security, make sure the latest operating systems (OSs) and company-licensed software are in place, and support remote workers — all of which means more work for IT staff. This IDC white paper examines some of the device management issues facing firms of all sizes, but especially small and medium-sized businesses (SMBs) with 200 or more technology users. The key pain points that firms need to address are discussed, and specific approaches that can help in client management are examined.

SITUATION OVERVIEW

The changing technology profile of firms and moves to enhance productivity make client management a major challenge. The empowerment of workers via access to advanced technology has made a difference in the improved financial performance of a growing number of firms. Coming off of the Great Recession of 2008, firms in the United States and across the globe, especially those in the SMB segment, made major changes in their organizational structure, trimming jobs and streamlining processes. This contributed to a rebound of revenues, but with lower head count. The pattern is expected to continue, with IT spending across company size categories growing at about two percentage points above GDP growth as firms depend on technology to drive their success.

IDC believes two technological developments drive enhanced worker efficiency: the growth of online resources and the empowerment of mobile workers. Organizations supporting employees who use their own technology in a bring-your-own-device (BYOD) environment are increasingly common around the world. The BYOD philosophy now extends to employer-funded technology that workers can use when they are away from the office in a choose-your-own-device (CYOD) approach. This development gives workers equity in the selection of a device even if company money rather than personal money is used for the purchase.

The expanding use of new technology has not come with an expansion of IT staff to provide support because resources are often divided between implementing new capabilities and keeping current technology operational. Firms of all sizes have a mix of IT spending priorities. Mobility and cloud resources are important, but upgrading PCs, improving network capabilities, and improving security are cited even more often as a spending priority over the next 12 months (see Table 1).

TABLE 1

Top IT Spending Priorities (% of Respondents)

	Small Business (<100 Employees) n = 500	Midsize Business (100–999 Employees) n = 310	Large Business (1,000+ Employees) n = 206
Upgrade PCs	45.4	38.8	37.0
Enhance servers/network infrastructure	11.4	33.1	39.4
Increase storage capacity/ improve storage management	11.3	24.3	36.9
Improve network security/ security management	17.3	31.4	38.0
Support for employee-owned devices/BYOD	4.3	15.1	22.7
Expand use of Google Apps/ free resources	10.3	4.2	7.9
Increase use of online/ off-premises resources	9.0	22.8	39.3

Note: BYOD and online resource interest grows with company size.

Source: IDC's *U.S. SMB Survey*, 2012

The continuing investment in advanced technology places even more pressure on IT staffs across various sizes of companies. Among small businesses, a full-time IT staff is often found in the majority of firms once they grow to 20 or more employees. But even as firms grow and increase the size of their IT staffs, the workload for each IT staff person only increases with each new technology innovation. Support for remote locations as well as remote workers means that a significant amount of IT staff time is spent simply keeping things running. Major projects and development work are prioritized in between putting out different fires that almost always flare up at the worst times. It's no wonder the IT department seems to be running as fast as possible without really making progress. Effective support for devices and the users who rely on them preserve precious IT resources for the kinds of assignments that can make a competitive difference rather than simple maintenance.

Company IT Pain Points: Acquire, Deploy, Manage, and Not Go Crazy!

For midsize firms, the pressure to improve productivity and performance is especially intense. They are in an awkward middle space, challenged from both above and below. They are being challenged from below by smaller firms that are more agile and more niche focused and able to provide higher levels of customer intimacy. Meanwhile, larger companies have more resources and access to more sophisticated technology solutions.

The changing nature of technology now requires IT organizations to provide ongoing support for local and remote employees while gearing up for the next round of technology deployment. The ideal situation is one with proactive engagement, where both technology and support can be regularly adjusted as appropriate. There are three key components to this process. Each component has its own challenges as well as potential for new technology to provide important assistance:

- ☐ **Technology acquisition.** Technology acquisition decisions are typically driven by the diverse mix of priorities noted previously. Investments may focus on new and innovative resources or on updating and maintaining the effective operation of what is already in place. The key is enhancing productivity and effectiveness. Even without a formal ROI analysis, senior management wants a good intuitive feel that IT investments will help workers be more successful in doing their jobs.

- ☐ **Technology deployment.** The coordination of technology in multiple locations is a major challenge for midsize firms, which typically do not have IT staffs in every location. Updating technology that everyone is supposed to be using, especially software or network resources, can be a significant chore, but online tools, including cloud capabilities or software as a service, lighten the burden.

- ☐ **Technology management.** The proliferation of company-liable and employee-liable devices made technology management a growing concern of IT staffs, with enforcement of evolving BYOD rules a very visible issue. This is where advanced systems manageability is very effective in meeting the needs of mobile workers as well as the company. An area of particular concern is providing critical security in the event that a device is lost or stolen. This, in turn, makes remote lock/wipe and remote find just two critical capabilities that can lower the risk of BYOD and push resources down into the hands of more and more mobile workers.

BENEFITS OF CLIENT MANAGEMENT SOFTWARE

Operating an effective IT organization requires IT executives to gain a deep understanding of the unique needs of the business and an ability to identify systems that are critical for operating its key functions. It is essential that IT staffs have a comprehensive view of the IT landscape to provide technologies that drive business efficiencies and allow them to properly manage their systems. IT executives must also ensure that proper governance and controls are implemented only where needed and with the least amount of restriction and interruptions to the business.

For IT organizations to remain relevant to the business, they must adapt to today's global and mobile workforce initiatives. As business needs and customer expectations of IT systems continue to grow in complexity and demand shifts closer to a near-real-time response, IT staffs must be able to leverage more centralized and automated solutions to effectively deliver their services. Client management software significantly aids IT organizations in reducing the total costs associated with managing PCs. By having the ability to maintain standardized hardware and software platforms, conclusive IT asset inventory records, and automated software distribution capabilities, IT organizations ensure that devices are optimized for both performance and security. Automated client management software reduces the costs associated with IT staffs relying on manual processes for systems accountability. Often, these manual processes are error prone and result in reduced business-user productivity and system security.

By implementing standardized system configurations in combination with a comprehensive PC management solution, IT organizations significantly reduce the labor costs and complexities related to device management. For example, IT organizations that leverage standardized configurations, robust IT asset management solutions, and automated software distribution capabilities find it less costly and cumbersome to implement conclusive system patch and vulnerability management programs. The ability to auto-discover devices and capture software inventory in order to populate and maintain an up-to-date and accurate IT asset management system is vital in establishing an effective device management program. This allows IT staffs to target the deployment of software to the right devices at the right time and reduce unnecessary system downtime.

In addition, a primary challenge that many IT organizations encounter with keeping devices on current software versions is preserving and migrating the business user's unique data and settings to ensure uninterrupted productivity when upgrading or replacing PCs. Often, IT staffs accomplish system software upgrades via attrition and/or manual processes. These processes are labor intensive, time consuming, and error prone and hinder the adoption of new technology. By automating these types of manual processes, IT staffs more efficiently ensure the stability of their systems and in turn shift more of their focus to providing strategic value to the business.

With businesses increasingly relying on rapidly changing technology to remain competitive, IT executives must be viewed as trusted advisors and offer IT services that are more proactive and less reactive. As businesses continue to expand their global footprint and embrace mobile workforce initiatives, IT staffs are likely to find traditional manual workflows too slow to respond to the cascade of real-time requests. Therefore, they must leverage service delivery tools that allow them to proactively monitor their IT environment and automate the distribution of software in order to optimize the performance and security of their systems. Furthermore, with mobility and globalization initiatives, it is becoming increasingly critical that IT systems have the most current software — including OS versions, system drivers, and security patches — to reduce data security vulnerabilities. Devices lacking the most up-to-date software and drivers are particularly susceptible to malicious attacks and/or data compromise.

#241489 ©2013 IDC

THE HP COMMERCIAL MANAGED IT APPROACH

As the divide narrows between corporate-owned and personal-owned devices as well as work and home offices, today's workforce expects to have access to corporate data on multiple devices anywhere at any time. This demand overwhelms IT staffs and increases the importance of their ability to leverage centralized IT systems management solutions and automated processes to manage, maintain, and protect greatly dispersed systems throughout their life cycle.

HP Commercial Managed IT (CMIT) solutions provide IT staffs with extended capabilities from software management to advanced hardware management and configuration. By leveraging centralized tools, IT staffs more effectively manage client devices from a single-pane-of-glass view. Furthermore, advanced automation capabilities allow IT executives to empower their customers with business-enabling technologies while reducing the efforts and costs associated with managing core IT functions.

The HP CMIT solutions provide a suite of products to enable automated support capabilities across key IT support functions related to client management. This support includes solutions targeting IT departments' vital pain points: OS deployments/migrations, mobile users, and device management and patching (BIOS, drivers, and software). HP recommends that IT departments leverage a solution that reduces not only software costs but also the total cost of ownership of the device. To accomplish this, HP partnered with and recommends LANDesk management solutions to provide the following capabilities:

☑ Acquisition and automated deployment of the most current HP drivers as well as hardware and firmware updates

☑ Configuration of BIOS and firmware settings on all HP devices in the environment to enforce security and power-saving settings

☑ Receipt of hardware health alerts to proactively resolve issues and/or remediate vulnerabilities

As a result of the rapid expansion of BYOD and mobile workforce initiatives, many IT organizations are increasingly challenged with effectively managing and securing the onslaught of devices entering the corporate environment. Therefore, many IT executives seek the value in offering their end users a device that they use as much as their personal tablet but that the IT department can fully manage and secure. To address this, HP launched the new CMIT Tablet PC line, which currently includes the HP EliteBook and the HP ElitePad Revolve, allowing IT administrators to fully manage HP tablets from within their PC management solution. These devices have been designed specifically for the commercial managed environment, with several manageability features such as network PXE boot, remote System BIOS setting changes, WMI support, and driver support.

To further extend the management capabilities, HP has also partnered with LANDesk to provide differentiated security capabilities for managing tablet devices. The LANDesk Management Suite eliminates the need for an additional mobile device management product, infrastructure, and knowledge base. These capabilities include:

- ☑ **Driver distribution.** The most up-to-date drivers to all HP CMIT Tablets (ElitePads) are distributed over the corporate network or remotely via Wi-Fi or 3G network.

- ☑ **Locate my device.** GPS coordinates, cell tower triangulation, and IP location enable a bird's-eye view map illustrating the location of lost or misplaced devices.

- ☑ **Remotely lock device.** Lost or misplaced devices can be "software locked" with password protection while the recovery process is instituted, helping ensure that company data is protected.

- ☑ **Erase confidential data.** For lost devices that are unable to be recovered, IT administrators can perform a reset, returning the device to the factory's or the company's gold image. To ensure greater peace of mind, IT administrators perform an irrecoverable wipe operation by remotely executing HP Remote Secure Erase, which clears all contents from the HP ElitePad's storage space, conforming to JEDEC Standard No. 84-A44.

- ☑ **Enforce geographic policies.** IT administrators can enforce hardware and software policies based on an employee's precise location. For example, IT staffs can set policies to disable USB ports or prevent access to certain applications when devices transition in and out of designated locations.

Additional Client Support

The HP and LANDesk partnership extends well beyond management of traditional PCs and the HP CMIT Tablet PC line. IT organizations also see a substantial return on their investment by managing nontraditional or niche devices provided by HP, including thin clients, retail point-of-sale devices, and high-powered workstations. The LANDesk solution understands the complexities of these devices, such as management of write filters on thin clients and tracking of and health alerts on peripherals attached to retail point-of-sale systems. For IT organizations supporting Android, iOS, or Windows Mobile devices in conjunction with their HP PC clients, HP also provides LANDesk Mobility Manager. All these solutions are integrated into a single console, enabling IT departments to streamline IT staff knowledge into only one tool rather than multiple solutions.

LANDesk allows IT administrators to automate the remote provisioning and management of Intel vPro functionality. With LANDesk, IT administrators can remotely activate their vPro-enabled devices without requiring physical presence. This allows the capability to both isolate virus-infected devices from the network with one click and remote boot devices to perform diagnostics or install images. In addition, "always available" management allows for the management of remote devices via out-of-band device discovery to enable inventory summary and power controls.

HP Hardware Management Integration in Other Client Management Solutions

The HP Client Integration Kit for Microsoft System Center Configuration Manager (SCCM) allows customers to streamline bare metal, no-touch deployment of client PCs as well as remote BIOS configuration. HP also provides HP Client Updates for Microsoft SCCM, which allow customers to view, download, and deploy HP drivers and updates from within their SCCM console. Furthermore, HP recently released HP Platform driver packs for each of its commercial PC systems, which enable SCCM users to streamline the deployment of required system drivers by packaging them all into a single distributable and extractable file.

HP also realizes that many customers today are not standardized on LANDesk or Microsoft SCCM and are content with continuing to leverage the investments they already made in other solutions. HP provides free utilities so that these customers can integrate advanced hardware management capabilities into their existing management toolset. These solutions include HP SoftPaq Download Manager for viewing, downloading, and installing applicable drivers and software applications to the customer's environment, HP System Software Manager for remotely deploying drivers and updates to systems, and BIOS Configuration Utility for remotely configuring firmware settings.

CHALLENGES AND OPPORTUNITIES

HP's approach of integrating hardware platforms with automated client device management solutions seeks to reduce the complexity and cost associated with delivering optimal IT systems and services to the business. This allows IT executives to focus less on keeping the lights on and more on becoming strategic business partners, driving technology adoptions that directly result in increased business efficiencies.

As a result of various factors to include company acquisitions and nonstandard IT practices, many IT organizations currently have a plethora of different desktop device types in their environments. Therefore, IT executives may find it challenging to take on the significant task of implementing and standardizing on a particular desktop hardware platform across their organizations.

In addition, the rapid increase in varying mobile device types entering the workplace drives the need for IT organizations to balance end-user empowerment with managing proper governance and control. As IT executives look to meet the complex challenges associated with mobility, many look toward leveraging point solutions for mobile device management to provide business users with a fuller range of functionality and IT administrators with advanced management capabilities.

SUMMARY AND CONCLUSION

IT organizations increasingly face the challenge of delivering IT services that empower business users and drive business efficiencies while maintaining proper governance and control. As the diversity of IT systems entering the workplace grows, so does the importance of the technologies that are leveraged by IT administrators to manage and support them. It is increasingly inefficient for IT organizations to rely on a cascade of decentralized tools and manual processes to manage the systems and software associated with providing both a secure and a user-centric IT environment.

To be effective business enablers, IT executives need to leverage solutions that increase the productivity of both business users and IT staff. IT organizations dedicate more time to driving business-impacting innovations by automating the timely and costly manual processes involved in systems management. Specifically, that automation includes security management, service management, and asset management, such as provisioning new desktops, patch/update management, OS migrations, and endpoint security. Automated and integrated IT systems management solutions are more essential for IT organizations to control the costs associated with providing the infrastructure, staff, and services needed to react quickly to support business initiatives and add new capabilities.