Is your enterprise ready to “Bring Your Own Computer”?

Introduction: The decade of Bring-Your-Own-Computer

In the next 18 months, a significant percentage of companies will likely give their employees a stipend for their own computer or device–a device which does not belong to the company, but belongs to the user. This model is often referred to as "Bring-Your-Own-Computer," or BYOC for short.

In early 2009, there were several articles written about Citrix's decision to give money to employees to buy their own laptop, rather than having one supplied by their company. Most of the articles were skeptical to some degree, with blogger Patrick Cunningham boldly stating that a bring-your-own-computer model is "penny wise and pound foolish." (One commenter more boldly states that it's "truly one of the worst corporate ideas I've ever heard.")

This paper will discuss the pros and cons of BYOC, and review the reactions—both internally and externally—in the first year after Citrix and Intel announced the BYOC model. One of the biggest proponents of BYOC is the Citrix technologist who coordinates the program, has been interviewed, as has the aforementioned Patrick Cunningham, one of the biggest dissenting voices. Perhaps most importantly, this paper will discuss the business, security, and technology issues that must be addressed for any BYOC program to be implemented successfully.

At visionapp, we believe that BYOC is an idea is going to take off this decade (and probably over the next 18 months) for the simple reason that users will demand it. The bring-your-own-computer concept is popular with young end users, who have grown up with a computer keyboard and who've never known a world without cell phones. These, after all, are the future rising stars, and they are the ones driving business for the future.

The pros: If you love your computer, you'll complain less

Citrix and Intel talked to the press about the concept of "Bring-Your-Own-Computer" in early 2009. Immediately, many members of the press—as well as many IT directors, who are Citrix and Intel's target customers—weren't sure why a company would choose to pay for a computer that belongs to the **user**, not the company.

According to Citrix, BYOC "will greatly increase user satisfaction by giving employees the freedom to choose the exact mix of options, features and styles that match their personality and individual computing needs."

Tedd Fox, a Technology Evangelist who coordinates the BYOC program for Citrix, explains the motives behind the model. "We designed the program for the Echo Generation," Fox says. " They are the people raised with TiVo and the Internet, who have lived online for a good chunk of their life. They know their way around a computer and usually have strong opinions about the laptop and OS they use. Most of the time, they have an awesome laptop that they love to use already." Although Citrix doesn't come out and say this directly, the thinking goes along these lines: **If you love your computer, you'll complain less.** That equates to fewer help-desk calls and

more productivity. I'm not sure if any companies have done a cost-benefit analysis taking this into account, but it makes a certain amount of intuitive sense.

Fox outlines many cost reductions in the BYOC model:

1. **No hardware help-desk calls.** Citrix requires 3-year coverage on all purchased laptops, and the employee deals directly with the laptop supplier, not with IT, when they have a hardware issue.
2. **Reduced inventory of laptops.** Fox says the company still maintains a fleet of loaner laptops for when employees have to send their laptops in for repair, but that they've been able to reduce their inventory because they do not need to maintain a fleet of laptops for new employees.
3. **Infrastructure savings.** In order for the BYOC model to meet all the HR and legal requirements, including Sarbanes-Oxley and other data security measures, Fox says that there was a lot of top-down planning involved. Citrix makes a lot of back-end software that supports a model where all the user's applications, resources, and data live offline, however, so I think the nature of their business probably made it easier for them to implement BYOC. This type of planning allowed Citrix to take advantage of the savings that technology like virtual desktops offer.

Fox reports that the first year of the program was successful. The roll-out of BYOC wasn't all at once–Citrix did it by geographic area, which also allowed them time to tailor the program to different countries' privacy and data security laws. Fox also points out that BYOC is not for everyone, and isn't required. "If users are happy with the [corporate-owned] laptop, support mechanisms, and need a bit of extra handholding," says Fox, "they can stay with the IT delivered device and service offerings."

Of course, Citrix doesn't need to pay for the software needed to modify their infrastructure to support BYOC. Their back-end infrastructure software that supports the BYOC model is free to them, which obviously positively affects their ROI. Other organizations would have to pay to change their infrastructure into something that can support this. There are many options available, of course–Citrix isn't the only player in the virtualization or management space. But Citrix's software outlay was probably significantly less than other companies.

The scariest trend in corporate America?

For all the press that Citrix and Intel have received around the BYOC concept, there are many detractors. Most of the public skepticism focuses on the assumptions that organizations aren't ready to deal with the policy and infrastructure changes they would need to make, and that the users would not accept the additional responsibilities of owning the computer themselves.

First of all—and Fox underscores this point often—BYOC is not for everyone. Trying to shoehorn BYOC into an organization where companies require corporate data to live on the user's hard drive probably doesn't make sense. "In effect, you have to quarantine the physical end point in some fashion and restrict information usage to a 'safe' computing arena that the organization can manage and maintain," says Patrick Cunningham, a long-time corporate records manager

and the author of Above the RIM, an information management blog. Cunningham has given a lot of thought to why BYOC is a Pandora's box. Cunningham believes that there are many thorny business issues that move to the forefront when a company implements a BYOC program. He explains that legal issues are the biggest problem, followed by security and investigation issues.

Some examples of problems created by BYOC are:

1. **Legal issues.** When internet access became more common in the workplace, some users accessed pornography online. In many jurisdictions, an employee who uses a work computer to access online pornography can create a hostile work environment, and the company can be sued if it does not address the issue properly. However, in the BYOC model, the computer belongs to the individual, not the company. How can the company be assured that a hostile work environment won't be created? The company can discuss the specifics (e.g., not on company time; not on company property — just like an individual can't bring their own copy of *Playboy* to work). The organization's legal and human resources departments have to spend time crafting a policy for this.
2. **Security and investigation issues.** When the computer belongs to the individual, how can the company stop proprietary information from falling into the wrong hands? With a work-owned laptop, the company can demand a full search of the laptop — remote or otherwise — at any time. When an individual owns the laptop, suddenly there are privacy issues. In the USA, individuals can be protected by the Fourth Amendment that prohibits unreasonable search and seizure.
3. **User troubleshooting issues.** Cunningham believes that IT departments can deliver a much better user experience than users who pick and configure their own laptops. He contemplates the difficulty of telling the office spreadsheet whizzes that "they have to turn off the corporate proxy setting when they go to Starbucks with their laptop." Cunningham concludes that if the IT department properly configures the laptop, it will reduce help desk calls much more than a BYOC program.

Although the BYOC program has been successful at Citrix, Fox believes that a BYOC program can't exist in a vacuum. "I cannot stress enough that planning and deep analysis is the imperative to a successful programme," says Fox. "We had many long discussions and meetings to make sure we took everything into consideration." That included bringing human resources, legal, and management into the planning sessions to craft policies that dealt with legal concerns and e-discovery.

Fox also agrees that IT had to change its approach over the way it delivered information to users. In Fox's case, the company provides the entire back-end infrastructure, and many, if not most, employees have all applications and data living in shared servers. Virtualization technology and "cloud computing" has made much of this possible.

"Remember the times before VPN?" says Fox. "People had to physically be in the office to work, because data had to stay inside the corporate walls. When VPN was introduced, IT people all over the world had these same concerns [legal, discovery, privacy]. The concept still took off because users wanted this functionality and IT made it happen."

My BYOC experience

I have been one of those employees who has fought hard at previous companies to buy a different kind of computer than the PC they wanted to give me. I researched and wrote pages of documentation about how my choice will save the company money and allow me to be more productive. In most cases, I've won, even when it meant running on a different OS than everyone else. But I was one of a small minority to even attempt it, and even now, looking back, I think the company gave in with a sigh because it was less trouble than continuing to fight me.

Conversely, in those instances when I had a corportate-owned PC that I didn't choose, I complained constantly. My biggest complaint: as a graphics manager, I constantly had to use special characters that I could only access through Windows Character Map. On the Mac—which is what I fought for and chose for myself—a quick character combination like option-shift-bracket or option-8 gave me what I needed almost instantly. On a Windows machine, I had to spend one or two minutes digging through the character map to find the typographer's quote or bullet. I am sure the IT help desk found my constant complaints annoying, and probably gritted their teeth every time my name showed up on their caller ID.

After I convinced the company to buy a Macintosh, I called our IT help desk considerably less. Part of the reason is that the help desk told me, "Yes, you can have a Mac, but we don't have Mac expertise. So if you have an issue, we probably can't solve it." But because I've been a Mac user since 1989, I was comfortable with that; with Windows, I didn't know a .dll from a hole in the ground, so I couldn't even begin to troubleshoot it.

My experience is one of the reasons why companies like Citrix have implemented the BYOC program—and their program looks quite a bit like the experience I had. By the way—when I left the company after six years, when my Mac was two years old, I bought the Mac from the company for a sharply reduced price. It was, in essence, like I had brought my own computer.

—Paul Ardoin

Cunningham still calls BYOC "one of the scariest trends in corporate America," but concedes that end users are demanding it and "the IT buzz is increasing every day." One thing both Fox and Cunningham agree on is that the IT architecture has to radically change to support the BYOC model. While Fox embraces the change, Cunningham sees the BYOC model requiring "an incredibly disruptive and restrictive environment"–in a program that's touting the freedom of choice.

The experts weigh in, but are they reflecting reality?

Like Citrix, Intel publicly pushed the BYOC concept. Intel blogger David Buchholz discussed BYOC on his IT@Intel blog, and in an IT Business Edge interview. But Buchholz still addressed BYOC from a conceptual, not a practical, level. Buchholz says that BYOC is "not ready for corporate prime time" yet. In Buchholz's examples, he assumes that the applications and resources that a user needs for their corporate work must run in isolation from their personal items. Like Cunningham, Buchholz has concerns that many users will have tremendous difficulty managing both their personal environment and the isolated environment.

Buchholz and Cunningham are two of many IT pundits who believe that BYOC means that security solutions and policies have to be layered on top of the current corporate PC and laptop model. That approach is fraught with problems — it's a band-aid solution at best, and a corporate nightmare at worst.

However, it's important to note that the current corporate PC and laptop model is layered on top of the 1980's model of PC's in the workplace. When the PC arrived in the early 1980's, each PC was a completely locked-down environment. You had to be at one single station in order to do your work, and almost always worked in isolation from every other PC in the building. As connectivity has been steadily opening up the corporation, IT has been stacking security and data solutions on top of that model for more than a decade. The "connected

isolation" model creates many shortfalls: users not backing up, hard drives getting corrupted, information being sent to the wrong people, viruses infecting systems, and so forth. All these shortfalls are due to the fact that the intrinsic model of the 1980's PC wasn't built to accommodate both full connectivity and full security.

If IT departments—and the pundits discussing the evils of BYOC—think their current IT model is adequately protecting company information and addressing privacy issues, chances are that they're wrong. A 2009 survey uncovered that most people simply don't follow their corporate security policies. About half access personal web-based e-mail accounts; three-quarters copy information onto portable storage devices to work on at home; more than half installed their own software onto their company-owned machine–**just like they would in a BYOC model**.
The reality is that IT departments need to make policy and infrastructure changes to support a BYOC model—because 80% of organizations out there have all the cons of a BYOC model today with none of the pros.

So what is needed on the IT side to adequately support this model? Yes — making significant changes to infrastructure does need to happen, and I think the IT leaders have to be willing to make these significant changes. This new approach has saved some organizations millions of dollars — something that can't be done by bootstrapping security and data products on top of today's corporate-owned model.

How do you make BYOC work in your organization?

This paper has discussed the pros and the cons of BYOC—and how many of today's organizations are using a model that has all of the cons of BYOC with none of the pros.

In summary, some of the pros are:

- Lower costs (PC inventory, help desk, purchasing)
- Attracting "Echo Generation" employees
- Happier employees
- Increased workforce mobility

Some of the cons are:

- Increased legal issues
- Conflict between company discovery and individual privacy
- Non-standard hardware: either end user or IT staff must be responsible for fixing problems

Those companies who have been successful implementing BYOC programs took two important steps:

1. They took on these potential "cons" in the company policy. HR, legal, and management sat down and banged out an information policy that addressed the legal, privacy, and e-discovery issues.
2. Secondly, they took a look at their infrastructure, and in some cases, completely redesigned it.

visionapp has assisted some of our clients to implement the BYOC model in various stages and variations. Those customers who redesigned their infrastructure made it possible for just about everyone to do all their work on a central network (like Citrix did). In those cases, the end users don't have to keep any applications or files on their laptop — they can stop in the middle of a task on their thin-client at work, drive home, and pick up where they left off on their home computer. Contractors and third-party partners can bring their own laptop to the company, and those workers have access to all the appropriate resources, but none of the company-proprietary resources.

Some technologists believe that BYOC can be successful if users run two virtual machines on the laptop — one personal, and one corporate. That approach has its use cases, and may be appropriate for some companies (and some end users). visionapp hasn't encountered a client who has had the exact same requirements as another client — sometimes one VDI vendor is the best for a client, sometimes another one is. Sometimes clients need a mix of application virtualization, streamed applications, hypervisors, and so forth. Sometimes the end users can be most productive on web-based portals; other times, a desktop approach works best. Sometimes the BYOC model isn't an exact fit, but using thin clients at the work site and mobile device access on the road or at home works best and has many of the positives of (and similarities to) a BYOC model.

As with any major project, this can require a significant up-front investment, but visionapp has seen that the return on that investment can be recaptured quickly. One enterprise clienteed invest more than $10 million up front, but they saved almost $50 million in IT operations costs over the first 36 months–well beyond BYOC savings. They've been able to save on server management costs, lower energy consumption, increase user productivity, and more—all because they implemented an infrastructure that could adequately support the BYOC model.

Some visionapp clients have told us in follow-up meetings that they should have made these infrastructure investments years ago. When our initial assessment determined that their employees were treating their company-owned laptop as a personal laptop anyway–like the aforementioned survey found–visionapp worked with the company to update their information access and security policies, and create an infrastructure that supported those policies. Obviously, all organizations are different. And obviously, the BYOC approach—as Citrix's Tedd Fox says—isn't for everyone. But more and more organizations are considering BYOC, and realizing that reworking their infrastructure can provide a lot more than BYOC savings.

Resources

1. Ponemon Institute/IronKey Survey, July 2009
2. BYOC Demystified: Part 1 / Part 2 / Part 3
3. Is the World Ready for BYOPC?
4. visionapp's BYOC approach
5. Case study: visionapp's approach with Barclays PLC (PDF, 233kb)
6. ZDNet: Bring Your Own Computer–Citrix's Experiment in Computing
7. Above the RIM: Bring Your Own Computer
8. Miami Herald: Bring Your Own Computer to Work?
9. WindowsITPro: Bring Your Own Computer

About the author

Paul Ardoin, the director of North American marketing for visionapp, has worked in the enterprise software industry for over a decade. He has spoken at InfoSecurity Europe, the eFinancial World Expo, and Government Technology Conferences. He has published several articles on networking, security, and technology marketing in publications such as *California Computer News* and *European Communications*.

Paul holds an M.B.A. in Marketing from the University of Phoenix and a B.A. in English from the University of California, Santa Barbara.

Much of the content in this paper first appeared in January 2010 on the North American visionapp blog at *visionapp.wordpress.com*.

For a BYOC assessment

If you'd like to schedule an assessment of your infrastructure, please contact visionapp.
In North America:

> e-mail infoUS@visionapp.com
> call +1 (530) 886-8800 x130

Disclaimer

Disclosure and Warranty

The information, concepts, and ideas contained in this document are the property of visionapp AG. No part of this document may be disclosed or reproduced in any form without written permission of visionapp AG. Any violation thereof will be pursued.

All brand names and product names used in this document are trademarks of their respective holders and are recognized as such.

Any product descriptions or representations in this document are for identification purposes only and are not to be construed as a warranty of specific properties or guarantee or warranty of any other type. visionapp shall assume no liability, either explicit or implied, for the documentation.

About visionapp

visionapp specializes in the design, implementation and operation of server-based infrastructure and portal solutions. The company provides unique products and services for optimization and cost-effective administration of Windows Terminal Server infrastructures. visionapp Application Delivery Management Suite including visionapp Server Management and visionapp Workspace Management as well as consulting and ASP services form the core business.

Further Information

visionapp AG
Head Office: Frankfurt am Main
Helfmann-Park 2
65760 Eschborn
Germany

visionapp North America
Sacramento office
12240 Herdal Drive, Suite 14
Auburn, CA 95603
USA
Toll-free: (877) 886-8802

web: www.visionapp.com