

  
accenture

*High performance. Delivered.*

This article originally appeared  
in the June 2010 issue of

Outlook

The journal of  
high-performance business

On the Edge

## IT 2015

By Kishore S. Swaminathan

Chief Scientist  
Accenture

IT's future will be determined by the imminent collision of assumptions about operating systems, networks and mobility.

• Consulting • Technology • Outsourcing

Ask IT pundits where information technology will be five years from now, and chances are they will invoke Moore's venerable law: In 2015, there will be more computers of every ilk, and they will be smaller, faster, cheaper. But in my view, the analogy of plate tectonics—the extremely slow geological process of continental drift that rearranges the earth's crust over millions of years—is more useful for gaining an understanding of where IT might be headed.

Today's IT paradigm rests on three broad sets of beliefs related to operating systems, networks and mobility. These "continents of beliefs" have been drifting separately over the years, but now they seem to be on a collision course.

It is this collision that will define the future of IT.

### The OS drift

In the early 1990s, the various PCs and their operating systems were designed to be *platforms*, providing the standard substrata of services for software developers and a standard application interface for users. Their designs involved assumptions that were valid at the time, but not anymore.

First, PC operating systems were designed to free computer users from the tyranny of centrally controlled mainframes. Users could tweak their PCs in various ways to personalize them. "Freedom" and "choice" were two of the most common words used in PC commercials of that time.

Second, PCs had so little computing power, memory and storage that the operating system—which is essentially computing overhead—had to be kept extremely skinny so that applications could run at a reasonable speed. As more capabilities became available, the basic design did not leave much room for graceful extensions—a mistake

the makers of mobile devices would make a decade later.

Third, because corporate networks were rare and Internet use even rarer, the PC had to be self-sufficient. It had its own file system for storing files, and slots, ports and drives to connect accessories.

Finally, PCs were big, heavy and unlikely to be moved around, ironically deriving their security from size and isolation.

Fast-forward. First came corporate networks, then the Internet. The very features that enabled individuals to have unlimited control over their personal computers became available to every unscrupulous hacker on the planet. Your "personal" computer could become anybody's "personal" computer.

A lot of quick fixes were in order: firewalls to stop the intruders, DMZs (demilitarized zones) to solve some of the problems caused by firewalls, proxy servers to mask the individual computers in a corporation, intranets (companywide file systems) to store those unique or rare pieces of company information and to share them across the enterprise.

Then a sleek, mobile laptop displaced the clunky desktop. Although it ran the same OS, same software, stored the same files, it could be easily carried just about anywhere—and just as easily left under the seat in an airplane. Further, a laptop, even a company-issued laptop, could not be presumed to be a trusted machine, since it spent a lot of time outside the company firewall and could pick up any number of beasties from the Internet that could then attack the company's IT system from the inside.

But instead of addressing the problem through fundamental redesign, we have slowly drifted to accommodate the PC, mostly with band-aid solu-

tions. For example, it's not unusual for companies to fill their employees' USB ports with epoxy to prevent data theft.

### The network drift

The network has had a similarly checkered history. In the 1990s, most companies owned their LANs, but these were slow. They used modems over standard telephone lines (in which case they paid long-distance phone charges) or special phone lines such as T1s (in which case they had limited bandwidth) for exchanging data across LANs.

Our tendency, therefore, has been to use the network as sparingly as possible. Individuals kept their data on their computers, using the network only for accessing external data, browsing the Web, or email. Companies designed their network topology to keep as much data traffic as possible in their LANs, both to avoid depending on a third party (the telephone company) and to avoid paying for long-distance bandwidth.

Even as it became the lifeblood for companies, the Internet was also a constant reminder that the more connected you are, the more vulnerable you are to catastrophe. Thus companies today stand behind an enormous data fortress of firewalls, traffic-sniffing security software and disaster recovery processes.

Meanwhile, network technology in general, and the Internet in particular, have evolved by leaps and bounds. First, more users today connect to their corporate network or the Internet through Wi-Fi or mobile telephone networks than through wires, which means that users have access to the Internet—and hence to your corporate network—from points well outside the control of a CIO.

Second, the Internet is no longer just a communication medium but is evolving into a computing platform in itself. Caching technologies embedded on the network itself and in modern browsers can help you use the Internet even if you are temporarily disconnected or the server you need to access is down.

While the ubiquity, availability and reliability of the Internet have dramatically improved, so has the sophistication of the threats posed by the Internet, in many cases stretching the capabilities of even the more advanced IT departments.

So as network technology and the Internet have evolved, many of our assumptions about the network—that being on the network means being tethered to a wire inside your firewall, that it's an unreliable communication medium, that a typical company has the wherewithal to secure it, etc.—are quickly becoming outmoded.

### The mobile phone drift

Most of the world still calls it a phone because the mobile device started its life as a voice communication device. With few subscribers and fewer cell towers, the earliest mobile phones were optimized for radio reception and battery life. During the first part of this decade, the subscriber base increased, more cell towers were built, and slowly the phone became a data communication device as well.

However, the phones from the major manufacturers were designed like consumer electronics devices, each with the idiosyncratic bells and whistles the manufacturer chose to put into that model. As more and more people started using their unique devices to access corporate networks, companies had to worry about security as well as support for multiple devices. IT shops did—and many still do—look at mobile devices as a different species of

animal than computers accessing their corporate networks.

In fact, modern mobile devices are not idiosyncratic consumer devices. They are built on well-established “platforms,” which means the user is no longer dependent on a few bells and whistles from the manufacturer but can install a wide range of third-party software. Further, mobile devices can now bypass the telephone company network and connect directly with corporate networks through Wi-Fi both for speed and security. With full-fledged, standards-based browsers, they can access any website without requiring that the website be specially designed for the mobile device.

As a result of all these developments, it’s no longer useful to think of a mobile device as a “phone.” They are computers—they are built on platforms, you can install software on them, they have web browsers—just in a different form. With the sales of so-called smartphones projected to exceed the sales of PCs by 2011, they are no longer an isolated nuisance for corporate IT departments but an integral part of their IT ecology.

### **When continents collide**

Why this elaborate analogy with plate tectonics and continental drift? First, to underscore the point that although technology moves rapidly, the next generation of IT will be shaped less by such rapidly moving forces as Moore’s Law and the falling cost of storage, and more by slow-moving forces—change in our underlying beliefs about operating systems, networks and mobile devices. Second, to underscore the point that while continental drift may be a slow process, when the collision occurs, it won’t be a matter of simple convergence—as most tech gurus predict—but of large-scale destruction and a complete rearrangement into a new landscape.

So what might IT look like in 2015?

Today’s typical corporate IT organization—its data centers and all the PCs used by its employees—is enclosed behind an enormous firewall. The PCs are almost always owned and managed by the corporation. Each PC has its own version of various corporate software, and possibly personal software loaded by individual users—much to the chagrin of the IT department. Almost all the corporate software—from email to ERP—is run in the corporate data center. All inbound and outbound traffic from the employees’ PCs is filtered by the firewall.

But by 2015, the firewall will have shrunk considerably, and will host only the most important company data and applications that are unique to the company. Employees will likely bring their own devices—computers, netbooks, tablets or whatever. All software and content will live in servers—sometimes inside the firewall, sometimes outside the firewall—that are centrally managed by the company. Company content may be temporarily cached in any user device, although it will never be permanently stored there. Commodity services—including hardware, software and business processes—will be provided by third parties.

How would a company support different devices? Most applications and content would be accessed through a standard browser—perhaps running HTML5—so that the application is isolated from the idiosyncrasies of the devices. And what about those employees who need specialized software or extra computing power to do their work? Such users will be supported through “desktop virtualization” technology that enables them to access their own dedicated computer with whatever specialized software they need (typically a virtual machine in a data center) from any device.

Although it may seem chaotic, this scenario provides a number of benefits that outweigh the discomfort CIOs feel about sourcing IT capabilities from outside the company.

First, when commodity processes and applications are sourced from the outside, a company is not constrained by fixed internal capacity but can contract and expand as business conditions dictate. Second, by providing applications through the browser or through desktop virtualization, a company can manage all software centrally and avoid the enormous overhead of managing thousands of PCs.

Third, the documents that the employees create reside in servers controlled by the company rather

than on users' devices, giving a company considerable access to its intellectual property and control over the security of the content. Finally, this scenario recognizes that individuals are as dependent on IT as companies are, and enabling them to carry a device of choice for personal use while still imposing centralized control on software and content for professional use creates a win-win situation.

This IT scenario may in fact enable IT departments to cater to their business needs much more than be constrained by the limitations of technology.\* To paraphrase Tolstoy, today all IT departments are unhappy in the same way; in the future, each IT department will be happy in its own unique way.

**Kishore S. Swaminathan** is based in Chicago.

[k.s.swaminathan@accenture.com](mailto:k.s.swaminathan@accenture.com)

*Outlook* is published by Accenture.  
© 2010 Accenture.  
All rights reserved.

The views and opinions in this article should not be viewed as professional advice with respect to your business.

Accenture, its logo, and High Performance Delivered are trademarks of Accenture.

The use herein of trademarks that may be owned by others is not an assertion of ownership of such trademarks by Accenture nor intended to imply an association between Accenture and the lawful owners of such trademarks.

For more information about Accenture, please visit [www.accenture.com](http://www.accenture.com)

\* Until now, IT departments have used standardization as a means of managing cost, security and the smooth running of IT operations. The emerging IT paradigm enables them to achieve these objectives through a different mechanism: centralization.