

# ***The consumerization of IT***

## **The next-generation CIO**

November 2011

Center for Technology  
and Innovation





---

## ***Table of contents***

---

### ***The heart of the matter*** **2**

#### ***The consumerization of IT is transforming the CIO role***

---

### ***An in-depth discussion*** **4**

#### ***An expression of a deeper shift in workplace expectations***

The consumerization of IT is really about societal change	5
The CIO challenge: Forging an adult relationship with users	6
How CIOs benefit from the consumerization of IT	9
A new IT architecture for a new business relationship	9
A framework for a CIO in the era of consumerized IT	12

---

### ***What this means for your business*** **18**

#### ***Consumerization isn't about technology management***

CIOs must embrace a democratic management approach	19
--	----

---

*The heart of the matter*

The consumerization of IT is transforming the CIO role

**Figure 1: Percentage of employees using smart mobile devices for business use**

Only **40%** of IT decision-makers say their organization's iWorkers are allowed to access non-work related websites.

But **70%** iWorkers polled say they are doing so at work.

Source: IDC information worker custom survey, business IT custom survey, sponsored by Unisys, May 2011

40%

70%

*Users' demands that they be allowed to use technologies of their own choosing isn't a fad that will fade. CIOs can't squelch these demands—nor should they. The consumerization of IT is a symptom of a shift in workplace expectations that has been brewing for years and is now reaching an inflection point.*

## A shift in the relationship

The “consumerization of IT”—defined as the use of technologies that can easily be provisioned by non-technologists—is a hot topic among CIOs these days. Many IT leaders like to think that today's challenges from users to allow iPhone, iPad, and Android devices instead of corporate-sanctioned BlackBerry or Windows Mobile smartphones, or to overlook departments deploying software-as-a-service (SaaS) applications, will diminish as users tire of their novelty. Microsoft's forthcoming Windows 8 is also likely to encourage the company's huge user population to use cloud and cross-device data-sharing, to use personal apps, and to use tablets for both business and personal purposes. Perhaps IT leaders believe that like PCs in the 1980s, IT will eventually corral them.

But those views are wrong. Today's consumerization of IT trend is the culmination of a fundamental shift in the relationship between employers and employees—especially professionals—that began four decades ago. This shift has only now worked its way into the world of enterprise technology. It's apparent to PwC that employees' demands to use their personally preferred mobile devices, personal computers, applications, social media, and cloud services represent a transformation in the relationship between the typical IT organization and the business as a whole.

PwC believes that, unfortunately, most CIOs are missing this larger trend because they view the problem as simply a question of what, if any, additional endpoint hardware and software technologies IT will support and what management, security, and compliance controls to put in place should it decide to do so. These CIOs and their IT organizations are,

at best, reactive: they agree to support an employee-supplied device or application after some group has pressed its will, and then manage by exception, adjusting policies to each new circumstance.

“The shift that's happening now is dramatic,” says Abbie Lundberg, president of business technology advisory firm Lundberg Media and former editor-in-chief of CIO magazine. And many CIOs are stuck in the middle. “On the one hand, the individuals who make up organizations are wanting to be empowered and saying, ‘I should be able to use these tools that make me more productive,’ while on the other side, it's not the CIO but the IT staff who are very accustomed to doing things in a very controlled and closed kind of way.”

**40%** of devices used to access business applications are personally owned by iWorkers, up from **30%** in 2010.

Source: IDC information worker custom survey, business IT custom survey, sponsored by Unisys, May 2011

To be successful, CIOs must be proactive. They must accept the inevitability of the consumerization trend and prepare for it by rethinking how they run IT. CIOs must forge new, collaborative relationships with users, give them freedom to make IT decisions, and teach them how to assume responsibility for those decisions. They must also rethink IT architecture and controls to focus on controlling—or loosening controls on—information, rather than enforcing hardware and application standards.

**This paper explains the fundamental drivers of IT consumerization and shows how the CIO can embrace that force for the good of both the enterprise and the user.**

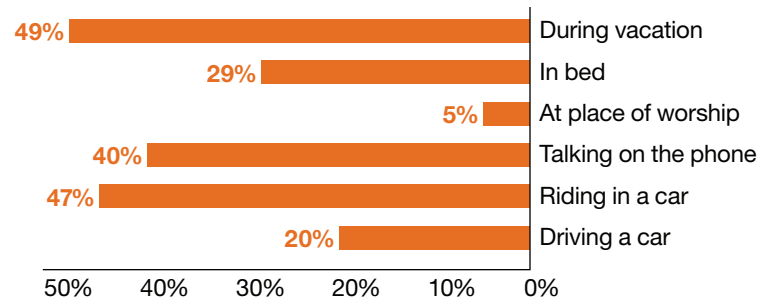
---

*An in-depth discussion*

An expression of a deeper shift  
in workplace expectations



**Figure 2: Most common places for work-related email, Tweeting, or posting to social media sites**



Source: IDC information worker custom survey, sponsored by Unisys, May 2011

## ***The consumerization of IT is really about societal change***

It's easy to blame vendors for the consumerization of IT. Blame Apple for inventing the iPhone and adding enough enterprise support to make executives refuse to take no for an answer when they want to use iPhone devices at work. Blame Facebook, Twitter, and Google for creating social and collaborative technologies that, once entrenched in employees' personal lives, became appealing for business. Blame salesforce.com for selling directly to business unit executives, intentionally bypassing IT, with the promise of fast, hassle-free deployments. Blame the inventors of hypertext and web browsers who created the ability for individuals to get information from anywhere. Go back even further, and blame Microsoft and Apple (again) for creating the PC ecosystem that, 30 years ago, started it all by letting people become familiar—even skilled—with computer technology at both work and home.

### ***The blame game***

The blame game misses the point, however, mistaking the manifestations of change for the underlying phenomenon. These technologies have expanded user expectations and abilities, and empowered users to act on their own. The fact that technology has become so personal and so easy to personalize encourages employees' desire to have "their" technology. Meanwhile, new capabilities can be provisioned at such low cost that individuals and business unit managers become encouraged to deploy trials quickly and, if they work, to expand them quickly. And because technology is so readily available to them, employees can often figure out how to bring it in whether or not IT approves—a dramatic change for many CIOs and their approaches to technology management and compliance.

But technology developments haven't caused the consumerization of IT. Consumerization of IT is an expression of a deeper shift in workplace expectations, especially among employees.

We believe that its roots lie in the social upheaval of the 1960s and 1970s that ushered in the notion that diversity is a positive force and that individual empowerment is good for business and society alike—ideas that stemmed from the shift in Western society after World War II. Soldiers returned home, but instead of going back to their farms or small towns, they moved to cities and suburbs, bought houses, and went to work for large companies.

---

## ***These trends then gave rise to corporate structures, work processes, management styles, and the work ethos that endure today.***

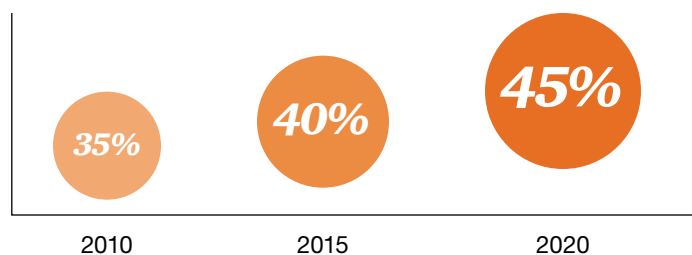
---

The added impetus for diversity and individual empowerment transformed the workplace even further, and by the 1980s resulted in flatter organizations with less middle management. In the same era, companies began to adopt quality circles and participative management approaches, leading to the rise of the contingent, distributed, and flexible workforce in the 1990s. In the 1950s, employees expected and relied on a long-term commitment to an employer. Now, in a new century, it's becoming more common for employees to be "nomads," preferring contractor status and taking responsibility for their own careers.

### ***The democratized workplace***

Employees wanted to feel like they were contributing meaningfully to their organizations—to have the workplace democratized, according to Julie Lynch, principal of Uncommon Consulting, which specializes in change management. Companies had to put processes in place that let workers participate in decisions. "And that's when you got the total quality management and quality circles," she said.

**Figure 3: The steady growth of Millennials in the workforce**  
By 2020, 45% of your workforce will be Millennials



Source: Forrester Research, Inc.

“You had customers co-creating products. You moved from the linear manufacturing management of a product to a kind of integrated chaos that was about the people. And because the pace of change continues to increase, we’ve moved even further down that integrated chaos line.”

That “integrated chaos” is now the norm at many companies. As a result, companies place greater emphasis on the value of individual contributions in professional jobs—promoting a meritocracy—as well as provide commensurate freedom of action. With freedom comes responsibility, but modern management gives professional workers lots of autonomy. The workplace is being democratized.

At the same time, the typical work environment no longer rigidly separates work and personal activities. As employers expected employees to be available as needed, companies created the infrastructures for mobile and work-at-home scenarios. That, in turn, led companies to allow personal activities at work to compensate for the loss of personal time outside of normal business hours. It shouldn’t be a surprise that employees want just one cell phone and the ability to use the tools they prefer across all their environments. Work tools have been democratized, too.

Now the tail end of the baby boomer generation that transformed the workplace is giving way to the next generation of managers who have ingrained expectations that they will control their work environment. And they now have direct access to the technology that lets them do so. This evolution can be neither controlled traditionally from the center nor ignored as inconsequential. “Some of the social dynamics underpinned by the changes in technology will fundamentally change the way that we view the world and the way that we interact,” says Mark Silver, the divisional CIO of Siemens Health Service.

If CIOs understand this context, they can create a more positive and supportive engagement with employees who insist on having “their” technology.

### ***The CIO challenge: Forging an adult relationship with users***

The fact is that personal computer technology is now entering its fifth decade—the late baby boomers and younger employees grew up with this technology, and many have never lived without it—and so people are more savvy about a wider range of technology than technology managers often give them credit.

### ***The right tools for the job***

It’s true that some employees don’t care about the technology they use; IT can provision these employees as before. But the ones who view technology as an extension of themselves will use their preferred technologies regardless of rules and guidelines to the contrary. CIOs need to engage them rather than have them fired or held to account, because they’re the same forward-thinkers who are likely to identify emerging business opportunities for the enterprise.

Many in IT seem reluctant to accept the existence of this new breed of employee; jokes about users correcting errors by using Wite-Out on their screens persist to this day, and “stupid user” stories remain crowd-pleasers in technology publications.

It’s true that most employees don’t have a sophisticated understanding of what technologists do. Employees are likely to be naïve about the work that goes on behind the scenes to make consumer technologies so effortless to use. And fewer understand the implications of supporting personal technology choices in a networked, process-oriented environment or the issues involved with integrating them with existing applications and infrastructures.





But that's no reason to protect employees from themselves as if they were babies trying to walk. CIOs need to forge an adult relationship with users. Like parents guiding adolescents, CIOs need to give users the knowledge and tools to make their own decisions and the room to make some mistakes—or risk poisoning their relationship. More independent users may take actions that CIOs and IT managers are not always comfortable with. But if the CIO doesn't let users do so, they'll never learn. Either the CIO will be stuck with a demanding infant forever—or with a teenager who gets more brazenly defiant as he or she chafes at restrictions. Neither outcome serves the CIO or the business.

This “parents of teenagers” mind-set is a difficult adjustment for many CIOs and IT managers, who are responsible for making sure nothing bad happens because of IT.

---

## Failure to ensure functioning business processes, compliance, and security has resulted in IT leaders being fired.

---

The role of the teenager, meanwhile, is difficult for many employees who believe they are more mature in these areas than they really are. But part of learning is exposure to consequences; as we all know, taking responsibility for our mistakes is a significant part of growing up.

It follows that employees—individually and as members of business departments—need to be held accountable for their behavior with technology, so that with the freedom they desire to directly deploy technology comes the responsibility to at least cause no harm to the company.

But all business leaders, not just the CIO, must accept such a paradigmatic change. “It's not just the CIO's conundrum. It's really management in general,” says change management consultant Lynch.

“Many company management teams cannot conceive of or perceive how their employees think about these social or collaborative processes enabled by the Internet platforms,” says Mike Willis, a partner at PwC and global XBRL leader with extensive experience in compliance and security efforts. “They did not grow up with them and are simply scared to death of relinquishing control of the processes to the masses.” Business executives faced with relinquishing control may take the attitude that inmates are taking over the asylum. But employees are not inmates, and thinking of them that way is a sure path to failure.

Yet CIOs rightfully fear that business staff will forget their promises when the novelty of controlling their own technology wears off or the burden of doing so becomes clear. When organizations execute change, says Lynch, most problems come from a lack of clarity about goals, roles, and process or the “lack of a strong and supportive performance practice that includes rewards and consequences.”

## Lessons from the field: The benefits to the CIO of the new paradigm

When CIOs talk about the consumerization of IT, they focus on what users want and whether that's supportable. There's less discussion about how consumerization could benefit the CIOs themselves by fostering greater satisfaction with IT among users, cutting costs, and creating an environment more conducive to solving business problems.

Companies have already discovered some benefits in the mobile context. Most companies in North America let knowledge workers use their own smartphones for work,<sup>1</sup> and businesses have discovered the cost and labor savings of letting employees self-provision and often pay (at least partially) for these devices—just as they did years earlier in letting employees pick their own broadband technologies to connect to office systems from home. (Remember when such high-speed connectivity was company-provisioned and -paid, just as at-home business faxes were two decades before that?) And CIOs who have endorsed device heterogeneity typically report that employees feel more productive—a perception that's valuable even if they're not.

Transportation communication engineering firm Arinc has long taken a liberal view on endpoint diversity, says CIO Richard Napolitano. “We generally had a model that allows as much freedom as possible within the constraints that we could afford to allow. We like that customer intimacy model, and we want to encourage it. And we have found that there is a huge—although intangible—benefit to allowing people to bring what they want,” he says.

One requirement of supporting heterogeneity was that it decrease overall costs, Napolitano notes. User self-support of the non-standard tools was often the means to accomplish that reduction. In the case of mobile devices, it also turned out that employees could usually get better prices from carriers than the enterprise could.

Employee-satisfaction and flexibility benefits accrue only indirectly to the CIO. A direct benefit of consumerization is the CIO's ability to turn “shadow IT” into “deputized IT.” CIOs of companies that have allowed Macintosh computers, for example, into their workplaces tell PwC that they typically find those users support themselves and each other. The same is true of iOS and Android mobile users, users of software as a service (SaaS) and other cloud services, and social networking users. That self-support reduces IT's support burden and identifies self-motivated business champions who can help promulgate good practices, be part of innovation and testing, and become de facto business technology analysts working with IT—not against it or in parallel to it.

In effect, extending IT decision making to users expands IT's reach and capabilities without requiring more IT staff—a real benefit given how much IT has needed to cut during the recent recession. The CIO gets a more detailed view of what's happening on the ground—where much innovation actually occurs—than can be accomplished when working largely at only the level of upper management.

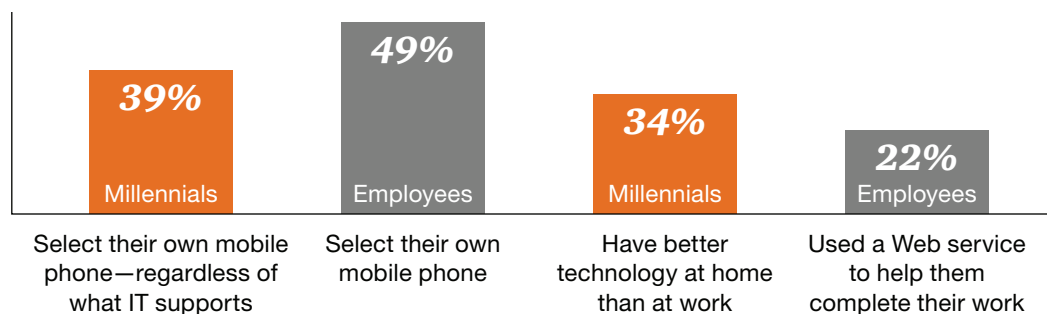
“For CIOs, that collaboration could be the compelling rallying cry to get both the businesspeople and the IT organization to come together to solve some of the problems caused by today's business pace,” says Abbie Lundberg, president of business technology advisory firm Lundberg Media and former editor-in-chief of CIO magazine. “We have to do things faster. And the old way of doing things is not going to deliver on that.”

At Arinc, the culture of acceptance for consumer devices has helped the CIO gain trust and the freedom that comes with it, Napolitano notes: “Three-quarters of the organization has come back to us and said, ‘Hey, the things you have done in the past have made my life easier. So I am willing to trust you to do it again in the future.’” That broad business-unit trust translates to trust and support at the CEO level as well, he adds, contributing to the success of the IT organization.

---

1 TJ Keitt with Matthew Brown, Ted Schadler, and Heather Martyn, Demystifying The Mobile Workforce, Forrester, June 7, 2011, [http://www.forrester.com/rb/Research/demystifying\\_mobile\\_workforce/q/id/59261/t/](http://www.forrester.com/rb/Research/demystifying_mobile_workforce/q/id/59261/t/)

**Figure 4: Business staff will expect to be more self-sufficient and empowered**



Source: Forrsights Workforce Employee Survey, Q3 2010

## ***How CIOs benefit from the consumerization of IT***

As employees and business unit leaders become more familiar with technology details, they will undertake more of the effort of putting together solutions for their individual and group business processes. That may seem like a loss for IT, but it's not. After all, the business units will not undertake the end-to-end focus on processes that extend across multiple business units and even enterprise boundaries. It is the end-to-end enterprise view that the CIO role will need to protect—and for which the CIO becomes better positioned when not focused on the tactical management of endpoints.

---

There will still be a need for infrastructure provisioning to serve the requirements of all business units, as they don't have the skills—nor the interest—to do so effectively.

---

IT organizations will retain the duty to build and manage the internal IT infrastructure and the externally provisioned services for enterprise applications (such as in a hybrid cloud approach)—even those that run at the business-unit level.

But the CIO's focus and mandate becomes more strategic: execute key business initiatives while enabling analytics, information exchange, and other activities that leverage the assets of the enterprise as a whole. And the relationship with the business units becomes one of strategic adviser and best-practices counsel, not perceived bureaucratic impediment. That relationship truly propels the CIO into the position of executive leadership that so many seek.

## ***A new IT architecture for a new business relationship***

Many CIOs and IT leaders blanch at the thought of employees creating or adopting a rat's nest of technologies that are poorly integrated, used in ways that create compliance and security risks, and eat up precious IT resources in an effort to contain the damage.

One reason for the fear is ignorance, says CIO adviser Lundberg. She sees only a small number of CIOs who both understand the value of IT consumerization and know technology well enough to understand the implications of giving users more control from the security and compliance point of view.

Lundberg says that CIOs who have extensive business experience but little technology experience are apt to underestimate the management and security issues when trying to accommodate the consumerization of IT, whereas CIOs who have had a strong operational focus tend to let a risk-avoidance mentality thwart legitimate flexibility. In both cases, the business suffers.

Any CIO who was professionally active in the early 1990s will remember the difficulty IT organizations endured to centralize and integrate the mishmash of technologies deployed by business departments in the years following the rise of the PC. It took more than a decade to rationalize organizations' technologies and supported processes—an investment CIOs don't want to see thrown out or to repeat as individuals and business departments assert technology ownership again.

Ironically, that will be exactly the result if CIOs try to treat the consumerization of IT as a contagion to be stamped out or quarantined. Studies by Aberdeen Group and others<sup>2</sup> show that such heavy-handed control both drives up costs and increases risks as employees work around corporate-sanctioned systems.

---

<sup>2</sup> Galen Gruman, "Mobile BYOD strategy reveals if your CIO is good or bad," InfoWorld, May 17, 2011, <http://www.infoworld.com/d/mobile-technology/mobile-byod-strategy-reveals-if-your-cio-good-or-bad-246>



PwC also believes that treating the consumerization of IT as a contagion will only isolate the CIO and the IT organization, driving IT into an operations-only ghetto that is at the greatest risk of being automated and outsourced (whether to the cloud or traditional vendors).

Conversely, we believe that a willingness to embrace, or at least tolerate, consumerization will help CIOs effectively support its legitimate aspects and, even more importantly, increase the strategic value of the CIO role to the business. Siemens Health Service's Silver describes that new role: "The role of the CIO is not to manage IT systems," he says. Rather, it is to help the business understand the information architecture that underpins its activities and, with business leaders as partners, "to document, clarify, optimize, and reengineer" business processes. In this role, the CIO has domain control over how the information used in those processes is stored, networked, and managed.

Part of that architecture rethink must involve many of the security and compliance policies and their expression in infrastructure choices that some IT professionals say are important to managing IT consumerization. The policies and technologies owned or managed by IT are part of the problem, says PwC's Willis. "It seems like most enterprises have IT infrastructures that reflect pre-Internet architectures and that are not well suited to meet the needs and expectations of interoperable, Internet-oriented architectures. These outdated architectures inhibit the very agility, collaboration, and coordination that consumers experience on the Internet and desire to use in the enterprise."

Within a new, open approach to devices and services there remains a requirement for CIOs to ensure that information is captured, organized, and secured but available to all the employees who would potentially use that information.

---

Letting users choose their own technology will create considerably more streams of information, which is ultimately good for the enterprise. The challenge for CIOs is to ensure that relevant systems and data continue to meet the standards of care and use for which IT continues to be responsible.

---

For example, IT will need to provide access to data that resides in core applications (such as enterprise resource planning [ERP] and customer relationship management [CRM]) and to ensure that new information generated in the now open environment finds its proper place in the enterprise information architecture. The traditional approach of a master database administrator—to enforce the architectural standards and data element definitions—must be modified toward a more flexible set of approaches. These flexible approaches should allow data to be captured or created outside the formal database processes, but be integrated by means of common definitions and standards. This type of dynamic, organic approach should replace a formal upfront control approach to database architecture.

Although there's no silver bullet that can deliver this result, we see frameworks emerging for CIOs to explore and adopt. The sooner you investigate them, the sooner you can turn the consumerization of IT phenomenon into a positive for yourself as CIO and for the organization you serve.



## How consumerization makes CIOs strategic leaders

A CIO who taps into the social and psychological shifts underlying the consumerization of IT trend becomes part of the strategic fabric of the organization. Nearly every business unit has its own needs and mix of technology interests. In many organizations, these needs are largely left unsatisfied due to limited IT resources and/or outdated IT infrastructure and architecture. Executive management steers IT to enterprise projects while business units perceive IT as a barrier to execution.

As a result, the IT organization is often separated from the company it serves and confined to core services such as enterprise resource planning (ERP), transaction management, networking, security, and e-mail that everyone depends on but doesn't necessarily perceive as strategic to them. Even CIOs who have IT staff working as analysts in business units tend to view technology in a siloed way: a strongly protected core and a periphery of isolated activities, experiments, or aberrations, depending on their tolerance of such projects.

This focus on the core—whether the result of management priorities or a CIO's own attention to big operational systems—warps the CIO view, divorcing the CIO from all the value-creating activities that happen in business units, such as sales, marketing, product development, customer support, distribution, and production. A good CIO doesn't let himself or herself get that isolated, but the nature of the core focus makes it difficult to have a deep view of the whole enterprise, especially those top-line activities that CEOs so much want to tap to gain revenue.

"First and foremost, CIOs need to be willing to give up the conventional stuff," says Rajan Nagarajan, until recently senior vice president at Mahindra Satyam, an IT services firm. "And they can do that in a smart way. But what seems to happen is CIOs keep gravitating to that conventional stuff because they love it; they will say, 'Oh look at this, I have a data center.'"

That ties them to only the non-strategic part of IT. Many CIOs react to such suggestions by saying how critical the back end is. And it is critical. But it's not the whole job nor is it strategic. "There's a split role for the CIO," says Mark Silver, CIO at Siemens Health Service. "One is to provide a policy framework, a process framework—to be responsible for information asset management, distributed data systems aggregation, and analytics. And then there's a piece of the CIO's business that's going to provide the core IT, such as the servers at the back end."

A CIO who has "IT deputies" throughout the business who choose their own technology can have a seat at the strategic front lines, better positioned to bring process, integration, and innovation skills to bear in places where a business benefit is more likely to be found than in the core.

"It should be a CIO strategy to go find those people, because they are valuable," advises Arinc CIO Richard Napolitano. Of course, the core must be well run, but a top-notch operations leader in IT should take on that role instead, as we've encouraged in previous papers in this series.

## ***A framework for CIOs in the era of consumerized IT***

If you're willing to accept that employees who want to use their favorite technology and related local processes should be given the opportunity, how do you safely and effectively provide that opportunity?

### ***The approach***

The methods PwC recommends are “soft” ones meant to address the social shift underlying IT consumerization. Although you'll no doubt create formal IT frameworks—for example, to determine security policies and methods for ensuring compliance with them—responding to consumerization with only technical policies and their related tools misses the point. Just as a user's desire for an iPhone or a Mac or OpenOffice is a manifestation of the underlying social shift that has occurred in the workplace, so too are choices of mobile management tools and data plan reimbursement levels manifestations of IT's behavior changing to align with that social shift.

Thus, to address that larger context, PwC has identified seven approaches that can help you shape your decisions about how IT will support consumerization.

### **1. View requests for support of personal or departmental technology as an indication that there is an opportunity for better results**

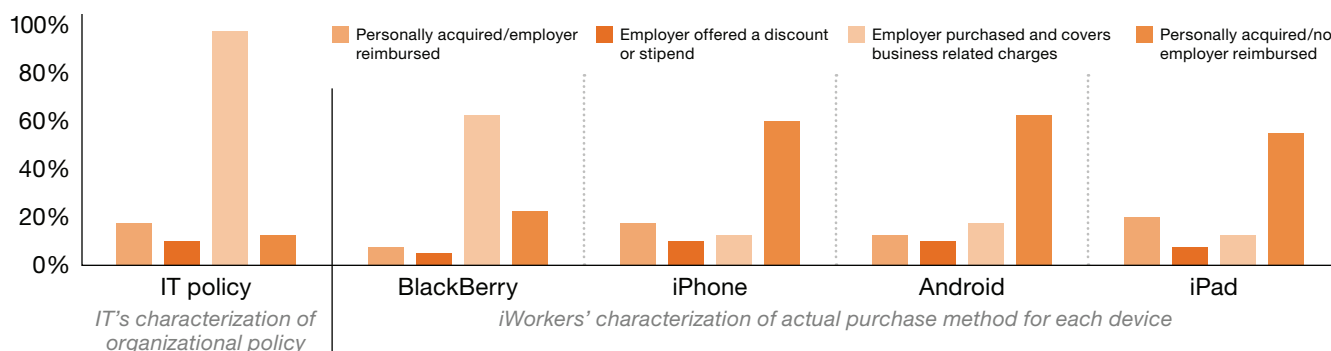
It's critical that you accept that the value of any technology may be in the eye of the beholder. Given that the business units are accountable for their success, they should get to judge that value. In other words, if the result of letting the business units use technology of their choosing is no worse than neutral, adopt a “let's see if we can support that” approach.

“The conversation at work is always about productivity,” not technology per se, says management consultant Lynch. The IT organization should help users determine whether what they want to do truly solves a problem. Ask users how a technology they want will help them, what their ultimate goal is, what obstacles prevent them from achieving it, and how their technology choice would change things.

Then ask yourself whether your current IT organization is positioned for, and has the skills to support, the technologies and processes that IT consumerization requires. Although the highest levels of competence in some emerging technologies may reside among users, the enterprise IT team must have at least a working knowledge of these technologies to ensure they can be integrated into the enterprise environment. In addition, new approaches to software development, deployment, and maintenance must be learned. And, though often overlooked, it's important for the personal, social, and political skills of the IT team to shift from command and control to become service oriented.



**Figure 5: Business staff will expect to be more self-sufficient and empowered**



Source: IDC information worker custom survey, business IT custom survey, sponsored by Unisys, May 2011

## 2. Promote the concept of shared ownership

The shared ownership approach is gaining traction in the mobile context, where employers let employees choose smartphones and tablets and use corporate resources if those choices can be managed consistently with IT security and management policies and processes.

In essence, in the shared ownership model, IT gets access to and appropriate control over the device to manage corporate applications and data, and the user gets control and rights to the device to install personal applications and access personal communications. Modern tools allow such co-management, but the real advantage is that this shared ownership approach reinforces the responsibility that the user or department assumes when it chooses technology, encouraging good behavior. For example, falling victim to a phishing attack on a personal smartphone might result in remedial actions, such as having enterprise data remotely erased or losing access to the corporate virtual private network (VPN).

Another issue in the shared ownership model is who pays for user and department-requested equipment: IT, the department, and/or the employee.

### Part of sharing ownership is taking responsibility for the costs you incur.

This is an accounting question, not an IT one, although IT may need to install the technology to manage the centralized accounting of these business-unit-approved individual expenses.

At Arinc, a transportation communications engineering firm, accounting for devices and telecommunications is managed centrally, “but it’s really distributed in terms of authorization,” says CIO Richard Napolitano.

Accounting for devices is another area where the IT management mind-set must shift from complete control to controlling only what is essential. The overall responsibility for the integrity of systems and data remains with the CIO regardless of how you partition work and responsibility for consumer devices and applications. You do not need to clean up the control issues that emerge, but you do need to ensure that users deploying new systems follow the guidelines you have put in place. That is part of the new responsibility that goes with their new freedom. You should work with your organization’s external auditors to determine and influence how they will assess IT in their work to accommodate consumerization. Do not accept the traditional standards of control, which hold IT fully responsible for what happens to user devices, and be prepared to establish new approaches and tools.

## 3. Assume heterogeneity

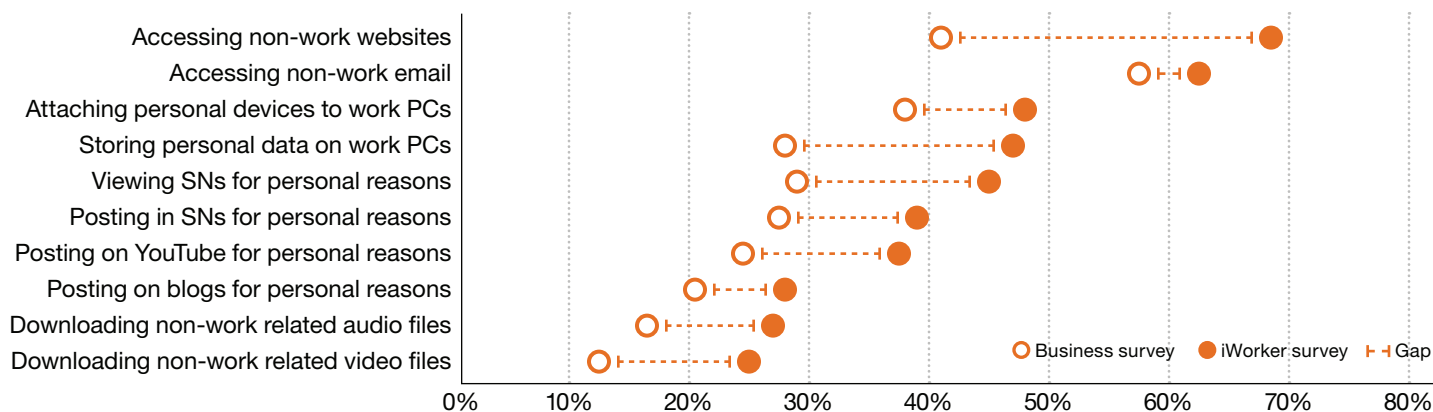
Whether the motivation derives from personal preferences or pursuit of actual business advantages, often multiple tools are available that are effective for a task or process. So why be limited to just one? For the IT organization, an assumption of device and application heterogeneity forces an architectural mind-set that is based on policies and processes, not specific technologies. Heterogeneity drives the architecture toward principles such as loose coupling that are themselves good things to strive for in support of enterprise agility.

Heterogeneity suits the times. Technologies change, vendors come and go, the business grows through acquisition or changes through divestitures, and business processes adapt to market and other forces. Support for heterogeneity allows you to easily adapt to new applications and deliver new capabilities. (For more on designing heterogeneous information systems, see the Summer 2009 issue of the PwC Technology Forecast, which focuses on “evergreen IT.”<sup>3</sup>)

<sup>3</sup> PwC Technology Forecast, Summer 2009, <http://www.pwc.com/us/en/technology-forecast/summer2009/index.jhtml>

**Figure 6: Activities enterprises currently permit**

Once again, the gap between what IT policies say employees can do—and what employees think they can do/are actually doing—is wide



Source: IDC information worker custom survey, business IT custom survey, sponsored by Unisys, May 2011

The Extensible Business Reporting Language (XBRL) is a good example of a heterogeneous approach. It provides a flexible framework inspired by the ease of use and ubiquity of the web's markup language to create a standardized approach for sharing, processing, analyzing, and presenting business information and related attributes. Information can be integrated across an organization while letting local business units use applications and technologies that work best in their local context. PwC's Willis suggests this style of collaborative, loosely coupled, orchestrated framework would apply equally well to other corporate processes—including IT processes—that involve heterogeneity. Enterprise architecture, technology architecture, service-oriented architecture, and IT Infrastructure Library (ITIL) version 3 also use similar concepts. The bottom line is that methods are available to support heterogeneity in a business-appropriate manner.

#### 4. View information systems as an onion

To view technology as a monolith, with each layer managed and controlled the same way, is folly. For this reason, policies are key to effective technology usage, allowing IT to manage the various devices, applications, and data across the many layers of the technology onion. Some require more control or security than others. Policies based on role, information type, and other key factors let IT ensure security and execute compliance across technologies commensurate with the risk for each factor.

Some organizations have taken one step in this direction by differentiating core and non-core activities, enabling users and departments to experiment outside the core enterprise systems (such as ERP) and data sets, while regulating the

interaction of any such information systems and the data they generate with those core systems. (PwC described this approach in the paper *The Value-Creating CIO*.<sup>4</sup>) This separation helps set the stage for a broader architectural change that abstracts information and processes from the tools and systems that act on and create them, and it formalizes the notion that non-IT employees are partners in choosing and managing the organization's technology and information systems—two key steps in adapting to IT consumerization.

#### 5. View control as a means to an end, not the end itself

Dealing with empowered individuals and co-ownership of technology processes likely sounds very messy to many CIOs, especially those who have been focused on operational efficiency, repeatable processes, and control-oriented compliance and security.

The key is to control only assets that are meaningful to control or what is legally required. Such assets may include information covered by privacy regulation, company trade secrets, and data related to transactions that need a validated audit trail or, in some more regulated situations, a precise chain of accuracy.

Whether by inclination or necessity, many CIOs have assumed the burden of control for the company—for control of business processes, outcomes from those processes, compliance, and security—and they assume that they must control anything new. Whether this approach stems from, at best, an attitude that “father knows best” or, at worst, the pretensions of a martinet, it's misguided.

<sup>4</sup> The Value-Creating CIO, PwC, 2010, <http://www.pwc.com/us/en/increasing-it-effectiveness/publications/the-value-creating-cio.jhtml>



Control is hardly the sole province of the CIO. Traditional management has long treated people as mechanical cogs, using various methods (some rewarding, some not) to enforce repeatable, machine-like activity, says Lynch. Although changes in management approaches since the 1970s have loosened such control in many knowledge-work environments and in some factories, it persists in many service and manufacturing industries—from fast-food service to call center operations, from truck delivery to food processing.

---

Today, IT systems often enforce such human mechanization, which may have reinforced a sense among employees that IT is about saying no—a perception a CIO may need to take into account.

---

Most managers are well trained in the linear predictability that makes for efficient, consistent operations, Lynch says. That's only half the skill set needed to effectively control the consumerization of IT. "You have linear predictability and product consistency on one side, which is necessary to run a business," Lynch explains. "And then you have this need for the integrated chaos that's people." That's where the notions of policies, risk and reward assessment, rewards, and consequences come into play.

Because you may need to adjust your policies along the way, it's also necessary to be a learning organization, says CIO adviser Lundberg. "You need to have in place a method to learn from the experiment and then apply that going forward."

## 6. Focus on intellectual assets first

As the locus of corporate computing has left corporate buildings and campuses, the notion of protecting information assets by using boundary security at the physical perimeter makes less and less sense. And this notion of protecting the physical perimeter is evaporating for more than just security. Given today's mix of employees, contractors, suppliers, and cloud-based services, business processes transcend boundaries. Thus, the business architecture a CIO manages, facilitates, and secures needs to start with information. "When you think about a business process, these processes they are trying to leverage and manipulate information assets. They are [also] creating them. That's what the intellectual property is in an organization," says Siemens Health Service's Silver.

For the CIO, this approach puts the emphasis on the "I"—information—in his or her title. "We are now looking at distributed data systems, many of which are outside of the organization's data systems," Silver says. "So the very idea of not having a standardized application or a standardized piece of hardware will be a nonsense argument in the end. We need to get to the point where we can validate the use of information sets. If we start to define the boundaries not as an infrastructure, not as a network, and not as a particular device, then really the boundary is any information data set."

Intellectual property can, for example, be standardized and thus managed more securely. PwC's Willis observes that the ModelWare platform at Morgan Stanley and the EDGAR Online I-Metrix system at the Securities and Exchange Commission update work processes that were characterized by thousands of electronic spreadsheet files and their inconsistent manually developed formulas created ad hoc by each user. To prevent such inconsistency, I-Metrix uses standard formulas and presentations—as part of an intellectual property library managed at the enterprise level—to enable collaboration among analysts. SEC analysts now use I-Metrix to review every company report for anomalies and accounting issues, ensuring consistent review despite the variance in skills and focus of each analyst.

## Solving the data security conundrum

CIOs seem to have a handle on securing sensitive files and information internally, within the confines of their corporate networks. However, once information exits the firewall (for example, enters the cloud), without a way to monitor or track it, companies are vulnerable to disastrous attacks.

CIOs need to be prepared to protect data as it moves outside the company boundaries. To do this, the data itself should be secured in an unobtrusive way. The common approach for any breach or hacking event is to target the file structure that forms the envelope around information. Modern IT security currently lacks the ability to embed security mechanisms directly into the information itself though traditional data loss prevention (DLP) tools are now being expanded beyond PCs to iPads and other mobile devices and can help extend centralized, broad monitoring to the new generation of devices.

New protection tools must be applied to fill this critical gap. When data breaches occur, immediate warning and detection can mean the difference between business as usual and potential catastrophe.

If files are tagged (for example, with visible and/or invisible digital watermarks), organizations can monitor and track those files when they travel outside of the corporate network, capturing detailed file usage activities in real time and alerting IT staff to unauthorized access immediately. Targeted scans of the Internet allow IT to pinpoint suspicious websites and peer-to-peer (P2P) sites that may house files that have been stolen and posted covertly.

File protection tools can also enforce usage rules for files by embedding specific policies that determine how a given file may be used, that limit who is allowed to open or forward such files, and that set limits on the number of files that may be downloaded from remote locations. In addition, the capability to disable or destroy files (based on geographic location or time, for example) is key to addressing a data breach. Having the ability to enforce such policies allows employees, partners, and others to share information safely and ensure that sensitive documents do not fall into the wrong hands, even as businesses operate in the cloud.



Siemens Health Service's Silver says that more and more chief information security officers (CISOs) understand this context for managing information assets, rather than endpoints. That should encourage CIOs who want to move the organization beyond the traditional endpoint homogeneity that is upended by the consumerization of IT trend. "The question is not 'How do we bludgeon everyone to death to use the same application?' but 'How do we manage risk using the plethora of applications that we have, and how do we manage data at the data level independent of the application, or the platform, or the hardware that it sits on?'" Silver says.

He foresees technologies such as data loss prevention and digital rights management being useful to manage valuable information assets, although these technologies are in their infancy today. But Silver also suggests that part of taking advantage of the consumerization of IT is to know when information assets don't need protection.

---

Sometimes, the value of an asset comes from being exploited for value-creating activities.

---

He cites the shift in the music industry, whose "protect the product at all costs" approach resulted in massive piracy that threatened the industry's businesses; now, a more flexible ecosystem involving a blend of digital rights management and open usage has emerged and the industry has at least stabilized.

The valuing of information assets isn't an IT problem. "This is a business problem," Silver says, and he cautions that CIOs alone cannot drive this mind-set change toward greater flexibility, even if IT can play a strong role in enabling it: "It can lead, it can cajole, it can manipulate, it can demonstrate value-add—IT does that anyway."

## **7. Remember, IT consumerization isn't really new**

Consumer technology has lapped at the enterprise shores for years. It used to be that photocopiers and fax machines were closely guarded, highly managed technologies; today, they are typically available for self-service. PCs were once limited to use by specialty workers, until they were adopted by almost anyone with a desk. And more importantly, the processes facilitated by each new technology became democratized as well.

"It reminds me of going from desktop publishing as a department in an organization to where everybody knows how to use PowerPoint. Or from when the finance folks were the only ones who knew how to use Excel, whereas now everybody's responsible for that," says Lynch. "Think about the graphic design piece. When people started to use those tools themselves, the concern at that time was, 'Oh my gosh, branding's going to go out the window.'" But business units and employees adapted, through standards, policies, education, and, yes, trial and error. The same is true of the technologies that IT owns today that are becoming democratized.

---

*What this means for your business*

Consumerization isn't about  
technology management



## CIOs must embrace a democratic management approach

A clear split divides those who are using the consumerization of IT as an opportunity to reinvent the CIO agenda. Some are now partnering very aggressively with the business, whereas others wish for the 1990s and are in complete denial about the change under way. The dot-com bust caused many to stop thinking of technology in only heroic terms, diminishing the value of CIOs at many organizations. Then came the recession and its big squeeze on technology innovation.

Now there's the consumerization of IT, which for many is the final straw in a period of ongoing turmoil among the CIO ranks. PwC has never seen so many CIOs looking to leave their current jobs because the role is no longer suitable for them, either because the role has turned into a "keep the lights on" role or because the role has become too transformational and they want comfort.

Ironically, the consumerization of IT could lead to both outcomes. It could push IT into the core and away from the business in some organizations. The trend also could challenge the CIO to be a transformation champion, leveraging the tech-savvy parts of the business and redefining the role of IT at the same time to one of stewardship more than operations. PwC believes the latter is necessary for most organizations, or will be in the coming years, but we know that the trail is still being blazed and the destination itself is more a hope than a certainty.

CIOs must get in front of the consumerization trend, says Vin Melvin, CIO of electronics manufacturer Arrow Electronics. "Ultimately, I have more faith in the core business principles adapting" to technology, he says, "than in technologists trying—in essence—to run the company through controls."

---

Consumerization isn't, ultimately, about technology management, and CIOs who think it is are fooling themselves.

---

Certainly, tools and practices will emerge that facilitate better management, security, and control of end-user technologies such as PCs, mobile devices, applications, and cloud-provisioned services. But those tools will be effective only if they work in the real world of users who have high expectations. The fact that the US military<sup>5,6</sup> and the National Security Agency<sup>7</sup> have decided that such consumerization of IT is not only inevitable, but can be supported, sends a strong message to CIOs in all industries that a new context for managing IT is emerging. Even a major security breach attributed to consumerized IT won't stop this trend in its tracks, notes consultant Lynch, because employees' demands to be listened to and trusted as an IT partner—to be empowered—are getting stronger with each generation.

"A seed will bloom in concrete in New York City," she says. And people "will not fit in a box on a line in the organization, whether it's networked or otherwise. They will find a way to bloom on their own. Humans will be unpredictable, and managers of any type—particularly IT managers and CIOs—will need to embrace this and educate themselves about it." Says Siemens Health Service's Silver, "Because of the power that people now have, you can't possibly make them widgets. They've almost become free agents within the system because we've empowered them so much."

---

5 Elizabeth Montalbano, "Army Selects Android For Mobile Battlefield Network," InformationWeek, April 22, 2011, <http://www.informationweek.com/news/government/mobile/229402123>

6 Nancy Gohring, "US Defense Department OKs Social Networking," IDG News, March 1, 2010, [http://www.pcworld.com/article/190457/us\\_defense\\_department\\_oks\\_social\\_networking.html](http://www.pcworld.com/article/190457/us_defense_department_oks_social_networking.html)

---

7 Gregg Keizer, "Apple calms concerns over volume Lion upgrades," Computerworld, June 20, 2011, <http://www.infoworld.com/d/applications/apple-calms-concerns-over-volume-lion-upgrades-759>

So the way to be successful as a CIO is to accept that fact. New research<sup>8</sup> in the psychology of work and in the neuropsychology of response to change helps show how, Lynch says: “What it boils down to is understanding and managing the self in terms of how do you respond to the necessity of inclusion, of collaborative decision making, of collective intelligence—that emotional intelligence piece that moves to understanding others.”

Investing in that kind of management and collaboration is essential to success in a workplace that seeks to get the most value from its employees’ varied strengths. And it’s essential for the CIO to be effective as more than a technology implementation and operations leader. “If you’re spending enough time building the human side of your organization, establishing trust, understanding what each other’s talents are, having that emotional intelligence or social intelligence, and then having a tolerance for mistakes, that’s what innovation takes,” Lynch advises.

Some CIOs are naturals at such management. Many are not and will need help—plus a senior IT management team that (a) accepts that the consumerization of IT is really about making people productive and (b) has the skills to manage an environment where diversity is the rule. “It comes back to being politically savvy and having good skills and leadership and risk management,” says CIO adviser Lundberg. “Of course, that’s easy to say and hard to do.” But expect it to be expected in the next few years.

PwC sees many organizations in the throes of this shift, dealing with it in a range of ways, from denial to embrace. Most organizations, though, are reactive. They’ll roll out a less restrictive mobile policy after salespeople and some managers each buy their own iPhone. Or they’ll turn a blind eye to the marketing team when it adopts a social networking tool, as long as no harm occurs.

---

## We recommend that CIOs—and business management as a whole—be proactive instead.

---

Rather than wait for rebellious employees to flout the rules, recognize that heterogeneity of technology is a strategic imperative and start deciding now which information assets must be controlled, standardized, and dictated. To do so, ask questions about which information needs to be protected, and in what processes and forms. Find out which tools—whether applications, devices, or services—are truly not interchangeable with others. Determine the domains in which users may be allowed to succeed or fail on their own because they bear the consequences and responsibilities for their actions, as well as gain the value of learning from their experiences. And figure out which risks require which levels of oversight and direct management.

Then map out the education, information architecture, and policies you need so you can adopt the new workplace order of individual empowerment and diversity—before you end up implementing them as a patchwork of exceptions. Getting ahead of consumerization will not only align your technology and management systems to the human reality, reducing friction, but it will also put you in a stronger position to lead technology and the business as a whole.

It won’t be easy, and like those organizations that reworked their hiring, promotion, schedule, and training policies in the past few decades to accommodate the diversity of employees and their individual circumstances, you may make some mistakes along the way. But the companies that led the way in shifting the approach to human resources management attained better results than those who resisted or ignored what employees wanted and needed to become more productive, happier contributors to the company’s success.

---

<sup>8</sup> See the “Inside Out” section of the article by Julie Lynch, “Engage from the inside out,” eMedia Vitals, April 25, 2011, <http://emediavitals.com/content/engage-inside-out>

# Sybase survey

July 2011

A survey by Sybase (*Device Disconnect: Companies Not Meeting the Mobile Workforce's Needs*, Sybase, an SAP company, July 2011) shows that although employees value the ability to perform their jobs from their smartphones or tablets, their companies have yet to meet their mobile needs.

The power to work from anywhere is closely tied to how satisfied employees are with their companies. Employers could use the following insights to better facilitate the mobile workforce:



59%

Almost six in ten workers believe that always being available on a mobile device is more likely to help them get ahead at work than coming in two hours earlier than they need to every day.



50%

Half believe that some mobile devices are better suited for the office, and others are more appropriate for use in their personal lives.



57%

Close to three in five report more technical problems with company-issued devices than those that employees supply themselves.



29%

Fewer than three in ten claim their company's IT departments are generally very good at managing mobile devices.



56%

The demand for better work-related mobile applications is high. A majority say that using mobile apps on the job makes them more productive.



27%

Less than three in ten are able to speak highly about their IT department's ability to set up or troubleshoot mobile applications or programs.



50%

Half would rather choose the mobile device they use at work than have the company in charge of this decision.

# Acknowledgments

## ***Advisory***

### **Sponsoring Principal**

Tom Degarmo  
Partner  
PricewaterhouseCoopers

### ***Us Thought Leadership***

#### **Partner-in-Charge**

Tom Craren  
Partner  
PricewaterhouseCoopers

## ***Center for Technology and Innovation***

### **Managing Editor**

Bo Parker  
Managing Director  
PricewaterhouseCoopers

### **Project Lead**

Terry Retter  
PricewaterhouseCoopers

### **Principal Author**

Galen Gruman  
Principal  
The Zango Group

### **Editorial Advisors**

Vinod Baya  
PricewaterhouseCoopers

Laurence Best  
PricewaterhouseCoopers

Bud Mathaisel  
PricewaterhouseCoopers

Alan Morrison  
PricewaterhouseCoopers

Terry Retter  
PricewaterhouseCoopers

## ***Copyeditors***

Lea Anne Bantsari  
PricewaterhouseCoopers  
Elana Varon  
PricewaterhouseCoopers

## ***Graphic Design***

### **Designers and Illustrators**

Samantha Patterson  
Sr. Designer  
PricewaterhouseCoopers

## ***Online***

### **Online Marketing Director**

Jack Teuber  
Managing Director  
PricewaterhouseCoopers

### **Designer and Producer**

Scott Schmidt  
Manager  
PricewaterhouseCoopers

### **Marketing**

Natalie Kontra  
Director  
PricewaterhouseCoopers

## ***Reviewers***

Laurence J. Best  
PricewaterhouseCoopers

Robert Kramer  
PricewaterhouseCoopers

Larry Marion  
Triangle-publishing

Justin R. Mcpherson  
PricewaterhouseCoopers

David A Stuckey  
PricewaterhouseCoopers

Christopher Wasden  
PricewaterhouseCoopers

## ***Contributing participants***

Abbie Lundberg  
President

Lundberg Media

Julie Lynch  
Principal  
Uncommon Consulting

Rajan Magaragan

Vincent Melvin  
CIO

Arrow Electronics

Richard Napolitano  
CIO  
ARINC

Mark Silver  
CIO  
Siemens Health Service

Mike Willis  
Partner  
PricewaterhouseCoopers

**To have a deeper conversation about  
how the consumerization of IT may  
affect your business, please contact:**

Tom Degarmo  
Partner  
PricewaterhouseCoopers  
267 330 2658  
[thomas.p.degarmo@us.pwc.com](mailto:thomas.p.degarmo@us.pwc.com)

Philip Garland  
Partner  
PricewaterhouseCoopers  
703 918 4523  
[philip.a.garland@us.pwc.com](mailto:philip.a.garland@us.pwc.com)

David A. Stuckey  
Partner  
PricewaterhouseCoopers  
203 539 4274  
[david.a.stuckey@us.pwc.com](mailto:david.a.stuckey@us.pwc.com)