# InfoWorld

# IT's consumerization *Special Report*

INTRODUCTION

# The iPad changed everything

## The tablet pushed the consumerization of IT trend in a way that IT can't stop

*By Nathan Clevenger*

WHEN EVALUATING THE ADOPTION OF MOBILE ENTERPRISE APPLICATIONS, it's important to understand the overall trends driving the adoption of the iPad within the enterprise. As I worked on the book "iPad in the Enterprise: Developing and Deploying Business Applications," I spoke to, interviewed, and received feedback from dozens of technology authors, industry analysts, enterprise software executives, Fortune 1000 CIOs, and other visionaries of enterprise IT. I felt that the best way to explore this concept was to hear from those industry leaders directly.

Although the iPad is an extremely polarizing topic on its own, the concept of the "consumerization of IT" is even more controversial. I spoke to nearly as many people who were unwilling to go on the record as to those who allowed me to quote them in the book.

The term "consumerization" first gained popularity in 2001 when it was used by Douglas Neal and John Taylor as a description for how information technology innovation was emerging in consumer-based technology, with the expectation it would eventually migrate into the enterprise.

## A SEA CHANGE IN THE IT/USER RELATIONSHIP

At first glance, the idea of consumerization might appear unlikely to have a big impact on the IT industry landscape and power structure of enterprise IT. Does consumerization really challenge the status quo of enterprise IT? Back in 2005, Gartner suggested it would.

That year, Gartner released a report saying, "The growing practice of introducing new technologies into consumer markets prior to industrial markets will be the most significant trend affecting information technology during the next 10 years."

In late 2010, Stephen Prentice, a Gartner fellow and vice president, wrote a Gartner CEO advisory titled "Seize the iPad Opportunity Now." But as early as 2005, he had written: "As perceptive CIOs seek to transform their rigid, legacy ridden infrastructures into agile, efficient, service-driven delivery mechanisms, they must adopt a pragmatic approach to managing the risks of consumer IT while embracing the benefits. Otherwise, the CIOs risk being sidelined as the 'enemy' by their constituencies."

In 2005, the idea promoted by Gartner that consumerization would be the most important trend of the next decade might have been controversial. But traction from the iPhone, which went from 0 percent adoption to 80 percent of Fortune 100 companies between June 2008 and June 2010, undeniably demonstrates the powerful impact of this trend.

Even so, Philippe Winthrop, founder and managing director of the Enterprise Mobility Foundation, believes that the mobile consumerization trend demonstrated by the iPhone (and now the iPad) is subtly different from the general trend of consumerization.

According to Winthrop, "The consumerization of enterprise mobility is slightly nuanced from the consumerization of general IT. First and foremost, the price points make mobile devices far more accessible than other computing devices. Second, the massive diversity of applications, and the ease of purchase and installation of these applications is very different from what IT departments are typically used to. Forward-thinking companies have recognized the opportunity to embrace, as opposed to fight, this change and use it to their advantage. True ROI is still elusive in many cases, but there is no question that the future of the workplace is predicated on the use of mobile devices and applications."

## HOW HYATT EMBRACED THE "CONSUMERIZATION OF IT" RELATIONSHIP

But what does the "consumerization of IT" actually mean to a corporate leader of information technology? In my search for a clear definition of this concept, one of the best explanations I've heard was from Mike Blake, the CIO of Hyatt Hotels. He shared with me the journey that

Hyatt went through to both recognize and then ultimately embrace this trend of consumerization with the iPad. In Blake's words:

"When iPad came out it was the latest "shiny object" introduced by one of the most innovative companies in the world. Everyone had to have one, yet no one really knew what it was for. The power in the product, aside from its beautiful design and solid operating system, was found in the spark that it created in the imagination of its users. Users were defining ways of leveraging the tool to prove that it is more than just flash, that it could offer true utility.

"In our case, IT embraced the iPad from day one, helping to get the product out into as many people's hands as possible. From that grassroots trial we have found ways of serving our customers in new ways, and providing powerful tools to our employees that they truly enjoy using. That's where consumerization of IT really comes into play. It is IT recognizing the power of a consumer product, cultivating it, and giving it a fair chance to succeed. We have shed our arrogance, but we keep a little bit of our skepticism and our conservative approach to make sure the enterprise systems are still secure and our help desks are not overwhelmed.

"IT's acceptance of consumerized technologies in the enterprise has led us to enable a more agile organization with users empowered with choice in selecting their computing platform preference. In fact, IT's embracing of these technologies has helped to propel a more positive view of IT. Where IT was previously considered to be rigid and dictatorial, it is now viewed as a true partner who proactively works with the business and uses consumer technologies to help solve critical business issues.

"The end result is that employees are able to get the data and information they need to better inform decisions. These consumerized tools enable people to better use and interpret information: they are easier to maintain, and have a higher satisfaction level with the user base than any previous generation of tools."

I believe Blake has demonstrated that the "consumerization of IT" is ultimately a positive trend for corporations. It may involve painful changes in the status quo of corporate IT, including, as Blake said, how IT groups have to "shed our arrogance" to give the underlying technology a chance to succeed. But this trend provides the business, the entire company, and even the whole economy with an improvement in efficiency, productivity, and profit.

## THE UPSIDE TO IT OF THE "CONSUMERIZATION OF IT" TREND

So how long has this consumerization trend been going on? Is the iPad acting as a catalyst, or has the trend been persisting for a while?

Scot Finnie, the editor-in-chief of Computerworld, believes that consumerization has been happening for a long time. He says, "The rise of consumerization of IT has become highly visible over the past several years. The immediate causes of the trend include the prevalence of powerful and versatile smartphones and tablets, the popularity of simple and useful mobile apps, and the recession, which has driven the need for greater levels of productivity and effectively longer workdays.

"Even so," Finnie continues, "the consumerization of IT has been evident for 20 years, beginning with the advent of the personal computer. Microsoft, for example, rose to dominance in the early 1990s in part on its intense focus on the end-user usability of its operating systems and applications. Apple, of course, has been a consumer electronics company for some time. The key for IT organizations is to recognize and embrace massive consumer trends, because they almost always manifest themselves in business environments, as well. Enterprises ignore or attempt to thwart the consumerization of IT at their own peril."

There is a big upside to the business if IT embraces consumerization. The upside is that the users themselves are bringing the latest technology into the company sooner than would otherwise happen. That can mean better integration, better communication, better tools, and ultimately a competitive advantage for the company.

Finnie offers hope to discouraged leaders: "At its core, the consumerization of IT is about employee freedom and employee productivity. At some point you have to just trust your employees and not only let them do their jobs better, but support them in doing so. The ROI will follow."

Donald Ferguson, CTO at CA Technologies, agrees with Finnie, saying, "The consumerization of IT has been gradually occurring for years. The iPhone followed by the iPad has made 'consumerized IT' the new normal. Enterprises can enable and support iPhone, iPad, and new consumer devices — or their employees will go around IT."

Frank Slootman, the former CEO at Data Domain and executive chairman of the BRS Division at EMC, shares similar sentiments: "Consumerization of IT is not a new

phenomenon with the emergence of the iPad or even the smartphone. As far back as the mid-1980s, the very first Macs and LaserWriters were ushered into departments of the enterprise completely against the tightly locked-down policies of the IT department who refused to support them. It is an unstoppable grassroots dynamic many decades underway. I am sure we ain't seen nothing yet."

## CONSUMER TECHNOLOGY NOW COMES IN THROUGH THE FRONT DOOR

Consumer technology is walking in the front door of the corporation, and Eric Openshaw, principal and vice chairman at Deloitte, says this trend is just as prevalent in the executive suite as it is on the front lines of the enterprise.

He observed, "The seemingly insatiable appetite for corporate adoption of tablets — and the iPad as a proxy for that broader adoption — reflects a fundamental shift from IT driving the how, when, what, and where of technology use toward the user dictating those parameters. It's fascinating that this is being driven both from the bottom up and the top down. In this case, people fresh out of school and CEOs alike have embraced an unobtrusive device that supports many if not all of their personal and professional computing needs."

According to Robert Stephens, founder of the Geek Squad and CTO at electronics retailer Best Buy, the iPad is facilitating an even more fundamental shift within the enterprise: user-driven design, which is driving improvements in business processes. "Up until recently," Stephens says, "most business executives didn't have any confidence to know what to ask IT for. But now they see that they can track a FedEx package right from the iPad, and see where it is or who signed for it. You can customize and order a pizza from Papa John's right from your iPhone. IT no longer has the unique set of knowledge about what is possible. The user now knows what they want, and they can and will demand it from IT."

Although the debate around the impact of consumerization will no doubt continue for some time, the adoption of mobile technologies and enterprise applications is moving forward, whether or not IT departments are on board.

Based on the opinions of those I spoke with, it is the role of IT to evaluate the opportunities that come with consumer technologies, weigh the risks and benefits, and define a strategic plan for the future. For those CIOs and IT managers new to the conversation, the good news is that it's a topic that everyone seems to be talking about.

*Nathan Clevenger is the author of "iPad in the Enterprise: Developing and Deploying Business Applications" (Wiley Publishing, 2011) and has been developing mobile software for more than 12 years.*

## Download the Consumerization Digital Spotlight



Once the euphoria has passed, real questions remain about the consumerization phenomenon. Even when IT gets over loss of control, legitimate and complex questions about risk must be addressed. And businesspeople soon discover that freedom of technology can descend into chaos without a framework to guide its use.

InfoWorld's "Consumerization Digital Spotlight" PDF special report walks you through the issues, opportunuties, and tools you need to adapt successfully to the consumerization trend.

Click here to download it now.

IMPLEMENTATION

# The real force behind COIT

## Business itself — not its employees —  drove the shift to employee-directed tech

*By Galen Gruman*

I HAVE YET TO MEET AN IT EXEC OR CIO FOR WHOM THE "CON-sumerization of IT" — employees asserting control over the technology they use for work — isn't now a major area of contemplation ... and sometimes consternation. But there's more to the trend than Apple-blinded employees bringing Macs, iPhones, and iPads into the office, even if they are the most identifiable champions of this trend. Let me take you through the key issues behind the consumerization — there's much more to it than mobile devices.

Two years ago, iPhones started appearing in the office, often connecting to corporate email and Wi-Fi networks. For many, that marked the beginning of the phenomenon known as the consumerization of IT, but it started years before the iPhone. People have been using their home PCs and Macs — systems not typically under strict IT management — for years, and Salesforce.com created a booming business selling cloud-based salesforce automation software directly to business execs, explicitly and proudly bypassing IT, half a decade ago.

As is usually the case with anything new, the IT reaction was to say no, and fears about security breaches quickly became the justifications for the policy. But just as with the home computer, public hotspot, and Salesforce.com phenomena that came before, the cost savings, lack of actual significant security problems, and executive joy at the new technology forced IT to move from "no" to "how."

### THE ROOTS STRETCH BACK TO THE 1960S

But anyone who believes the consumerization phenom-enon is driven by just technology is missing the point. The real change — and why it's ultimately not an IT decision — is in business itself. The 1950s were the pinnacle of the hierar-chical, military-style "company man" business — a conse-quence of the mass of military-trained World War II soldiers returning to the workforce. Then came the 1960s and 1970s, where individuals asserted their rights as individuals and as members of minority and other groups. The 1980s saw a deconstruction of the corporation into a flatter model, with fewer middle managers and more employee empowerment.

In manufacturing, this became highly codified, using tech-niques from management gurus such as W. Edwards Dem-ing, including the use of Lean and Six Sigma coupled with employee co-ownership in the form of quality circles and Toyota's "anyone can stop the assembly line" philosophy. The 1990s and 2000s saw a continuing hollowing out of middle management, the introduction of part-time and contract labor forces, and the replacement of routine work with robots, software, and offshore workers (in societies that largely had no individual-empowerment culture).

That left many companies with a smaller set of knowledge workers retained because they could think for themselves, as well as use their intuition, personal skills, and so on, whether for sales, customer service, product design, or operations.

### THE NEW WORKFORCE FAVORS THOSE WHO RELY ON THEMSELVES

The result is a workforce of nomads who come together as needed, using a wide range of resources in a variety of loca-tions. Inevitably, that nomadism accentuates the importance of the tools these employees use to do the work they're valued for. As each person's individual strengths vary, so do the tools they prefer to use — and begin to insist on using.

This phenomenon is by no means unique to knowledge workers. Many tradespeople — contractors and chefs, for example — have long used their own equipment because of the perceived better fit, quality, and/or feel. Software, comput-ing devices, and the like are the knowledge worker's equiva-lent.

Given these fundamental shifts in both business structures and the type of value desired from individual employees, a rift has developed between those new realities and the struc-tures that live on from the "company man" era. For example, employees are told to manage all or most of their retirement savings and to keep up their skills on their own dime and time. The company may help a bit, but it no longer takes care of employees in these ways. The notion of a job mar-riage, where doing your job meant lifelong employment and a secure retirement, is gone.

Thus, the relationship between the employee and employer has changed to one of ad hoc participation. As long as it makes sense for both the employee and employer, the relationship stands. When either decides the relationship is no longer desired, it's over.

## THE CLASH BETWEEN OLD & NEW CREATES THE CLASH BETWEEN USERS & IT

Yet the old "company man" approach lives on in IT and other operational systems. One example is the notion of a standard technology environment, where PCs and their software are reliably stamped out in identical units like cookies in a Mothers factory. The other is the notion that employees need to be protected from risk, by having it removed via technology wherever possible.

In other words, whereas employees are told to act like adults when it comes to their retirement and skills, they're treated like babies when it comes to technology usage.

As workers are told to be more independent and self-supporting, they're fenced in at home. Abbie Lundberg, the former editor in chief of CIO magazine and now a technology management consultant, has a great analogy for this situation: IT, the CSO, the legal department, and often HR treat business employees as babies who they lock in the house so that they don't crawl out into the street and get killed.

The better metaphor, she says, is to think of business staff as teenagers who are going to drive the car whether you want them to or not. It's better to teach them how to drive and set limits and expectations such as having a curfew and no-consequences permission to call for help if they do get in trouble.

The truth is that if you fence them in, they will find a way out. And that is what will get them — and the company — in trouble. Remember, today's knowledge workers are valued for their creativity and drive, and their technology familiarity lets them act on it in the realm once the sanctum of IT.

## MANY IN IT ARE LIVING IN A FOOL'S PARADISE

The uncomfortable reality for IT and business executives is that most are operating in a fool's paradise when it comes to the consumerization trend. A recent IDC study shows that although 40 percent of IT decision makers say they let employees access corporate information from employee-owned devices, 70 percent of employees say they access corporate data that way. That means in many organizations IT has no real handle on what is actually happening in the systems it is managing. IDC's research also shows that the use of personally owned devices is only growing.

Other IDC research shows the IT disconnect from the already-consumerized technology reality in their companies. There is a mismatch between IT's and users' views of policies relating to who pays for mobile services: IT thinks that the business determines and directly pays for business-related access, a view shared only by BlackBerry users (those whom IT provisions). Users of other mobile platforms say they bear the costs or charge them to the company as an expense — and thus make the decisions. In other words, these IT organizations see only the BlackBerrys that represent the pre-consumerization state of their organizations.

Forrester Research says that the consumerization trend will only intensify as the Millennials become a greater proportion of the workforce. In 2010, a quarter of employees were Millennials, a proportion that rises to 40 percent in 2020. Think about it: The Boomers who grew up in the individual-empowerment era of the 1960s and 1970s are largely the ones who have the political clout and financial ability to use their own technologies, but the generations that follow see such technology as simply normal.

I've heard several CIOs at large, conservative enterprises say they had to allow iOS and Android devices because "kids" wouldn't work for a firm that forced them to use a BlackBerry and Windows XP PC. The U.S. Army is a great example; it's proactively looking to deploy Android devices and iPads, and it's training troops on appropriate use of iPhones and other such devices because its 20-something workforce uses them anyhow.

One more study, this time from Aberdeen Research: The more you try to control employee-oriented technology, the more it costs you and the less safe you are. Remember that analogy of trying to fence in teenagers? That's why: When you rigidly control the technology and processes of knowledge workers, they actively work around you — and against you. Your "secured" email ends up getting forwarded to Gmail and Hotmail accounts where you have zero control or visibility into it. Documents find their ways onto CD-Rs, thumb drives, and cloud storage for transfer to home computers and from there to mobile devices. Cloud apps will be used more and more, as IT becomes viewed as the obstacle to getting work done.

The real shocker to me was the fact that a free-for-all envi-

ronment is safer and cheaper than a rigidly controlled one. But it made sense after Aberdeen researcher Andrew Borg explained it: If employees aren't actively fighting IT, they're less likely to cause issues. And of course the safest, cheapest approach is the "wise parent" approach: Use a mix of policies, incentives, and education to help your teen become a self-sufficient adult. The incentive is the right to use a device of their own choosing; the policies channel that use in safe ways, and education helps both reduce resistance to some burdensome but truly necessary policies and increase self-vigilance by the employee — the overwhelmingly vast majority of whom want to do the right thing for them and their company, after all.

## HOW IT CAN ADJUST TO THE NEW REALITY, WITHOUT ENDANGERING THE BUSINESS

So how does IT function in this new world? PwC came up with a frameworkd, which I think is right (both because I contributed to it and because it's enjoyed a good reaction when I've made this presentation to various IT audiences). The full PwC report laying out this framework is available as a free download.

It's a different way for many in IT to think, as it starts with "soft" values and requires IT to share ownership of risk management and technology decision making with employees and their business departments. (It requires the same of the legal, executive, and HR teams.) But as the consumerization trend is fueled by "soft" human issues, it only makes sense that the management response to it be grounded in human approaches.

On the technology side, the framework favors policies, not rigid barriers, to steer employees to the right outcomes while allowing appropriate freedom and creativity. It says the IT monoculture at the endpoint level is a dead direction, so IT instead should think of technology as an onion with multiple layers. The outer, employee-oriented layers should be flexible and individualizable, while core systems should be standardized and safeguarded as much as possible. A simple illustration: Allow any mobile device that conforms to your routine information access policies, but add layers of authentication and security measures such as encryption for those information resources that are truly sensitive within the network. Even if you let an employee access their workgroup share drive from an iPad doesn't mean that same employee can open your HR database.

The bad news is that not all the technology is available to manage this onion skin — the notion of information rights management is rarely implemented in typical enterprise data objects or systems, and rarely in user apps and devices. The good news is that by shifting risk from an IT- or CSO-only job to a shared one, you incentivize the business to reduce that risk through other means.

The other good news is that consumerization is not new. The first IBM PC or Apple IIe owned by an employee or department started this journey. The Internet pushed it to a whole new level, as information became unbounded, not just computing capability. Yet organizations have not only survived, they've thrived with that new power. Think back to the notion that Internet access had to be strictly controlled; it once seemed necessary and scary, but ended up not being so bad. Then you adapted as it became clear you had to, finding many positives to exploit along the way. Now apply that thinking to this newest set of waves: mobile, cloud, and social media.

*Galen Gruman is executive editor of InfoWorld for features, as well as its Mobile Edge blogger and Smart User blogger, author of "Mac OS X Lion Bible," and lead author of "Exploring iPad 2 for Dummies." Follow Galen's mobile musings on Twitter at MobileGalen and at Google+.*

IMPLEMENTATION

# Stay ahead of consumerization

Provide a framework for your users and they'll do your grunt work for you

*By Eric Knorr*

IT NEEDS TO LEAD AND TAKE ADVANTAGE OF THE NEW TREND IN consumerization of IT.

I'm not the first to say this, but the parallels between today's consumerization trend and the very early days of PCs are striking. From a user standpoint, the PC was about personal empowerment: The technology to do my job better is available on the open market and the IT department, which seems to care little about my needs, is not going to stop me from getting it.

If I recall correctly, way back when, the IT organizations that were quickest to embrace and lead the adoption of PCs gained the advantage — not only over IT shops that fought the new desktop paradigm, but also over those that rolled out PC technology willy-nilly. The same will be true of consumerization.

## A NEW RELATIONSHIP WITH USERS

The key for IT is to provide a framework within which users can procure their own stuff. Rather than users getting out of hand and messing things up, they can actually help take technology to the next level — and do much of the work to get there themselves.

The trick is to treat users as if they were part of IT. In fact, they already are. The majority of security breaches, for example, are caused by users who unwittingly download stuff they shouldn't. Users are the front line in protecting the security of the organization. If they felt like they were part of something, rather than simply following someone else's rules, they might be more careful.

If users are going to get more capabilities on their own, they need to accept the responsibility that comes with that greater empowerment. Rather than the consumerization of IT diminishing IT's power, it makes users conscripts to the IT cause.

If employees want to use their own smartphones for company email, for example, they need to accept that their device will forever be password protected — and if the device is lost, it will be wiped remotely. IT can set up the process, so users can provision their devices in this way on their own. The business gets added productivity with almost no additional overhead.

## DO-IT-YOURSELF TECHNOLOGY

In many companies this DIY model may soon extend to the user's primary computer. It's quite possible, for example, that Windows 8 will include a client-side hypervisor [5], which will be able to run a secure virtual machine containing everything the user needs in the way of business apps for work. When the system powers down, the business virtual machine goes away.

The main criterion for client hardware, then, is that it must be able to run the virtual machine. That's a wide range of hardware — so why not let the user choose? The company reimburses the user for the cost of the machine, but vendor tech support takes care of maintaining it — curing one of IT's biggest headaches.

The cloud side of consumerization is more complicated. Cloud services and applications need vetting to screen out providers with poor security practices and to avoid subscriptions that are redundant or wasteful. One interesting approach I've seen is VMware's Horizon App Manager, which gives users access to SaaS and Web apps, but allows IT to enforce policy — for compliance, among other things — and track usage.

You don't need to contemplate cloud apps very long to see the limitations of the consumerization of IT. Individuals should not simply run off and subscribe to stuff, and cost, security, and compliance aren't the only reasons. Even more important is data integration with applications already running in the enterprise. Otherwise, users are reinventing silos that fragment data about customers, products, projects, and so on.

So the long-range challenge for IT is to provide a consumer-like experience and enable users to self-provision through IT. In some cases, this may result in a certain class of user becoming more rather than less technical, as they cus-

tomize SaaS apps and maybe even aid with simple integration. But IT must always provide a rational framework.

The trade-off is clear: IT relaxes control over a certain part of end-user technology consumption, while in exchange end-users take on some low-level IT tasks while adhering to explicit guidelines. But for this new relationship to work, IT must also be attuned to the new capabilities users want and have a fast-track process to get highly desirable new products or services on the approved list.

## THE LIMITS OF CONSUMERIZATION

The consumerization of IT is mainly about adding capabilities around the edges rather than replacing core functions — nor does it have anything to do with the core application development that forms much of the intellectual property held by larger organizations. IT people do more than stand up servers and install software. They ensure everything works together, that people don't duplicate effort, that priorities are straight, that there's a plan and a point to the money being spent on technology.

But the surest way to cause chaos is to go overboard on control and try to stand in the way of consumerization. You can't win that battle because users will find a way around your prohibition — and you'll be left with a mess to clean up. One the other hand, if you provide the right framework and leadership, you have a shot at enjoying one of the rarest combinations in IT: more capabilities, less work, and happy users.

*Eric Knorr is editor in chief at InfoWorld and has been with the publication since 2003. A technology journalist since the start of the PC era, he has developed content to serve the needs of IT professionals for the past decade.*

## 10 products changing the business world

*From Siri and SSD to augmented reality and Ice Cream Sandwich, here are 10 technology game-changers.*



NFC, SSD, ICS, HTML5, AR, "The Cloud": Tech jargon can drive a sane person bonkers. Products based on these trendy acronyms and buzzwords are altering the business landscape at breakneck speed.

Want to know what they mean, why they matter, and what you should do about them? Read on.

**IMPLEMENTATION**

# IT's guide to consumerization

## Use businesses' know-how when you embrace consumer technology

*By Bob Violino*

As your organization moves to consumer-based technologies such as tablets and smartphones, cloud services, a mix of PCs and Macs, and social networking, here are critical practices to help create the right environment to make both IT and the business happy.

### CONSUMERIZATION STEP 1: CREATE A CULTURE THAT LIKES CONSUMER TECH

How can your organization ensure it gets the most out of consumerization and users have the freedom they need while at the same time maintaining appropriate control?

Perhaps the first move the organization needs to make is adjust its cultural orientation and attitudes from one of zero tolerance on consumer technologies to one of intellectual curiosity and business opportunity, says Frank Petersmark, former CIO of Amerisure and now a CIO advocate at the consulting firm X by 2.

Instead of automatically frowning on, say, employees bringing their own devices to work, you might think about how best to leverage this new technology and the processes that come with it for better customer service, improved profitability, or increased productivity, Petersmark says. An organization's ingrained culture is probably one of the biggest inhibitors to effectively and sensibly leveraging the opportunities presented by technology consumerization.

Part of the cultural change is getting IT out of the mind-set that only technology people can make technology choices.

For example, the IT team at the Austin (Texas) Convention Center had a hard time accepting that consumer products such as iPads would be suitable for use in its business environment, says Joe Gonzales, IT services manager. "In our organization, there is this perception that if a product didn't get ordered from our Dell Premier page, then it's not good enough to use in the enterprise."

First, the center had to get to a way of thinking that the objective is to give employees productivity tools, and it doesn't matter if these tools are considered business IT or consumer

IT. Now, it uses iPads to deliver service-order information to its employees on the show floor, and about 50 employees are using their own smartphones to access email and calendar information.

### CONSUMERIZATION STEP 2: FOCUS ON POLICY-BASED GOVERNANCE

This may seem obvious, but it's usually a big gap for companies to bridge: Develop policies to govern how consumer technologies can be used in the workplace, and deploy an asset management strategy for company-owned objects such as PCs and mobile devices.

Yes, consumer IT is largely about giving people freedom to choose devices and applications. But without a cohesive policy in place, anarchy can result.

"The majority of IT departments feel powerless when it comes to consumerization or any aspect of bring-your-own-device," says Barb Rembiesa, CEO of the International Association of IT Asset Managers (IAITAM). But governing policies, strong processes, and proactive guidelines will give organizations the ability to move into a consumer IT environment while bringing value instead of adding risk and cost.

Also, think about deploying IT asset management systems to control risk and ensure financial return of company-owned technology goods. After all, you own them because you have an explicit expected benefit or payback, or a specific security need that moved you to mandate that tool.

Your standard deployment process for technology may not accommodate the management of consumer technologies. For example, the Austin Convention Center found that its IT-initiated approach of adding a mobile device to a Windows domain and adding user profiles didn't address the casual nature of BYOD usage. The IT department had to start from scratch and determine how it was going to manage equipment, yet still comply with the City of Austin's IT security policies and procedures under which it operated.

In the end, the center wrote a new deployment policy that centered around educating users on the do's and don'ts

of device usage, Gonzales says. This is also how the center goes about segmenting company data and personal data on devices: by educating users about how not to mix the two.

IT also took responsibility for the initial setup of devices, so it could control app deployment on them.

## CONSUMERIZATION STEP 3: IMPLEMENT MOBILE DEVICE MANAGEMENT

Mobile device management (MDM) software secures, monitors, and supports mobile devices. Typical functionality includes app distribution, configuration and enforcement of access controls, and — for higher security environments — imposing usage requirements, such as disabling the camera or limiting Wi-Fi access to specified access points. Such software — and the policies they execute — apply to both company- and employee-owned devices.

Consider the experience of furnishings company Holly Hunt's iPad trial, where a few sales staffers used Apple iPads on visits to client sites. During the pilot, the company discovered there was no way for IT manage the updates of iPad applications without going through an iTunes account. That meant it had to have one corporate iTunes account for each device issued and users had to periodically send their device in for the company to update with the PCs running that iTunes instance.

This was an operational nightmare, says Neil Goodrich, director of business analytics and technology at Holly Hunt. Instead, the company decided to shift to a BYOD model for the sales rollout, eliminating the concern about IT needing to keep devices current. Users took that responsibility, aided by iOS's application alert system.

Holly Hunt also deployed MDM software, so it can blacklist certain applications where appropriate. It can also remotely wipe data and deny network access to devices that do not adhere to corporate policies.

This strategy gave the company what it wanted with its mobile strategy: Users can self-update their personal devices and get the full utility from the one device for both their personal and work need, and Holly Hunt can protect itself against risks such as lost or stolen devices.

In addition, MDM software allows for multiple profiles, so the company can have one profile for employee-owned devices and other profiles for corporate-owned devices, which it uses in its warehouse and fabrication facilities. Other organizations implement such multiple profiles to vary permis-

sions and privileges based on users' roles.

## CONSUMERIZATION STEP 4: TAP INTO YOUR EMPLOYEE BASE FOR APP IDEAS

For application development and deployment and the kinds of apps employees are allowed to use, many organizations are trying to catch up with the consumer marketplace, says X by 2 consultant Petersmark.

Most new employees enter an organization with a more capable set of productivity and networking tools, not just devices, than supplied by their new employer, Petersmark says. It's problematic at best and catastrophic at worst from a talent recruiting and retention perspective "if the best and the brightest decide that their new employer's infrastructure and application portfolio is far inferior to what they already have in their pockets," he says.

Forward-thinking companies are trying to embrace those in their organization who tend to push the boundaries on the consumerization front. Rather than considering those people to be troublemakers, Petersmark advocates that you bring them into the planning and deployment process and ask them why they use the devices, services, and apps that they do, how they use them, what benefits they derive, and so on.

Consider creating a small team of the more cutting-edge employees and ask them to help re-create some of the core application functions the company uses in the form of more consumer-friendly technologies, Petersmark says.

## CONSUMERIZATION STEP 5: GET OVER SECURITY SKITTISHNESS AROUND BYOD

Most organizations historically denied network and data access to anything that was not company-issued. But that doesn't work in a consumerization context. Thus, companies are increasingly creating secure access points via virtualization or cloud services that allow employees to safely access company resources with their own devices.

If done correctly, this tactic can yield several benefits, Petersmark says, including allowing employees to be more productive and maybe even more innovative by permitting some flexibility in how, when, and from where they are allowed to engage the company's resources.

Still, security remains one of the biggest concerns among IT executives when it comes to consumer technology in the workplace. Although some of the fear is fueled by vendors and analyst reports seeking to sell security tools, some of the wor-

ries are legitimate. But with tools for encryption and access control, you should be able to safely provide access to some enterprise data and applications to trusted users.

The adoption of a virtualization strategy addresses many of the challenges of consumerization of IT, says Paul Martine, CIO of Citrix Systems, a virtualization technology provider. By hosting all applications, virtual desktops, and data in the data center, you can deliver these services to any consumer devices in a controlled and secure fashion.

However, many virtual desktops are designed for use on Windows PCs and Macs, and they don't work well in a mobile environment. The issue is not just screen size, but lack of support for touch and other native user interface methods, as well as back-end applications that don't reformat themselves to the current context, says Ryan McCune, senior innovation director at Avanade. He notes that Citrix and others now offer APIs to help developers make their back-end apps mobile-savvy, so they can adapt to the device being used.

Cloud services that are designed to deliver apps and data securely over a network can also help address security concerns. But few cloud services yet work well with mobile devices; Google Docs and Microsoft Office 365 being prime examples of such PC-oriented services.

And many apps make it easy to use cloud storage services — such as Appe's iCloud, Box.net, Dropbox, and Microsoft SkyDrive — that IT can't manage. However, more options are emerging to make consumer-class cloud storage more palatable to IT.

## CONSUMERIZATION STEP 6: BUILD AN APP STORE THAT APPEALS TO USERS

People who use mobile devices such as iPhones, Galaxys, and Droids are accustomed to going to app stores to easily download what they need for their devices.

For its own employees, Avanade is developing several enterprisewide mobile applications, including some that will connect employee mobile devices into the company's social computing capabilities such as employee profile pages, microblogging sites, video and media sharing, search, communities, and blogs.

The majority of enterprise applications are not optimized for mobile devices, and many users opt for work-arounds to access them, says Chris Miller, Avanade's CIO. "We can take lessons from the consumer app store model and apply that to meet the specific needs of the business environment," Miller says. On the commercial software front, both SAP and Oracle have invested in creating mobile clients to access their ERP and CRM systems, in recognition of the increasing endpoint diversity among users.

An enterprise app store should provide employees with a central portal to request an application across any number of devices — from laptops and desktops to tablets and smartphones, Miller says. From a management perspective, it should also have built-in approval processes and workflows to manage costs and make sure the right people and teams are getting access to the tools they need.

And, says Avanade's McCune, enterprise app stores need to acknowledge the commercial apps available to users and steer them to preferred apps by adding links to the Apple App Store, Google Android Market, Microsoft Windows Store, and so on.

## CONSUMERIZATION IS UNSTOPPABLE, BUT THAT'S OK

The consumer IT trend seems unstoppable, given the proliferation of tablets and smartphones, cloud tools, social tools, and mobile apps in the workplace. That doesn't necessarily have to be a bad thing for technology executives.

Rather than looking at this development as another drain on IT's time and resources, organizations can embrace the opportunity to give workers new levels of productivity and flexibility, with the ability to work from virtually anywhere using the tools of their choosing.

If you understand your organization's risk tolerance and approach consumerization not as a threat but as a different way of managing, you can come up with an effective strategy that accounts for risk but also enables employees — and, in turn, enables your business. The returns can be substantial.

*Bob Violino is a freelance writer who covers a variety of technology and business topics. He can be reached at bviolino@optonline.net.*

IMPLEMENTATION

# 5 technologies users must own

## Giving users control helps IT avoid unnecessary work, support users better

*By Galen Gruman*

CONSUMERIZATION OF IT IS ABOUT USER-DRIVEN TECHNOLOGY of all sorts. BYOD has the distinction of being so visible and inexorable that it finally forced the consumerization trend into the open, with CIOs and IT publicly confronting an issue that many had been dealing with quietly for a while: Some technologies are truly user-centric and should be left as such.

Others have implications on the back end, where IT needs to be involved. Often, however, IT is told or tempted to get involved in every technology, which is a Sisyphean task it can't afford. IT must step back, first to understand what technologies users are owning and to determine where which really need IT involvement.

What technologies precisely are those in the empowered employees' quiver? There are five: mobile devices, cloud computing services, social technology, exploratory analytics, and specialty apps (that is, apps for the user's specific job, from presentation software to engineering calculators). Some research firms don't include the last one, and some add video to the mix — a perennial prediction that's simply a communications format and not a tool in its own right like the others.

The list is short, but the tools that fall into these categories are many. If IT realized these categories, it might be better able to anticipate where user-driven technologies will come into play, as well as understand the underlying rationale for them. For example, smartphones and tablets make information of all varieties more accessible, they make computing more portable, and they make all sorts of communication easier in more contexts. Exploratory analytics — especially when tapping into external unstructured data and big data sources to supplement the knowledge kept within the company — let business users look for and theorize about possible market shifts and opportunities that maybe would increase revenues or decrease expenses.

### THE COMMON ASPECT IS THE INDIVIDUAL NATURE

These technologies share two key aspects.

For starters, they're very personal, with users choosing the ones that fit their work style, user experience preferences, and ways of thinking. IT often ignores the fact that people think differently, and that artisans of all stripes have always had personal favorite tools that simply work better for them — or seem to, which is the same thing at the end of the day. Just as chefs and construction workers, doctors and sculptors have favorite tools that both reflect them and extend them, so too now can information workers. That's why you get heated arguments over Android versus iOS, or folks who swear by mind mapping and those who just don't get it. They're all right because they're all different.

The other common aspect is that they are all directly applied to the work at hand. They're front-end technlogies, not back-end ones. Individuals use them to accomplish what they've been hired to accomplish, and that individual ownership — expertise, really — reflects the person's history and experiences that have made him or her good at the job.

In other words, they are idiosyncratic technologies — very much the oppoosite of the standardized, almost robotic technologies that IT has been tasked to deliver in the name of efficiency and repeatability, which is why there is often such a clash between IT and empowered users.

With that in mind, all of a sudden IT can see that these tools are not ignorant choices or trivial demands, though they may seem so at times — but that's beside the point. Instead, they are reflections of the individual and his or her approach to work. That's the point: users choosing tools they believe help them do better at whatever they do.

Understanding this nature of consumerized technology can help IT distinguish the tools as expressions of individuals from the underlying principles and common actions that IT can deliver, aid, and augment through back-end technologies and through flexible governance around data and processes. And it can help both business and IT pros get past the control divide by realizing that like everything else, the technologies in use cover a range from highly specialzied and individual to highly standardized and universal.

## BEWARE SMOTHERING INDIVIDUAL TOOLS WITH LARGER SYSTEMS

Where IT also has to be careful is in trying to wrap these individual technologies in a blanket of back-end technologies. In many cases, it will smother the tools' individual, local nature — and cost a lot of money and time in the process. In other cases, it's easy to create parallel information systems — one for "regular" IT and one for "consumerized" IT — and end up with a big mess. For example, Forrester Research recently identified 16 technologies to support consumerization. To me, the list is misguided, proposing more areas where IT can spend money and time in an era when budgets are shrinking and demands on IT are already too high.

Here's what Forrester suggests IT should look into: business collaboration, client management suites, file syncing, infrastructure as a service (IaaS), innovation management and ideation platforms, mobile device management (MDM), platform as a service (PaaS), productivity, public social media, security and identity management, self-service BI, smartphones, social marketing management tools, tablets, videoconferencing, and video platforms.

Some elements on that list have long been or should be in IT's charter: business collaboration, client management suites, file syncing, IaaS, mobile device management (which is just an aspect of overall client management), PaaS, security and identity management, and self-service BI. These are all platform technologies that either enable or govern enterprisewide activities. Certainly there are aspects of these — I'm thinking cloud and multidevice file sharing — where IT can help adjust to new use cases and new endpoints, but they should not be treated as divorced from traditional information technologies and processes.

Other elements are faddish: innovation management and ideation platforms, videoconferencing, and video platforms. I've been hearing about the promise of video chats and video in business for two decades — they can have their place, but they are niche technologies that should get only niche attention, probably at the department level. Innovation platforms

come and go in terms of vendor attention; there are some industries where they can be helpful, assuming there is an innovation process to be aided through technology, but in many more situations, they are just more process for the sake of process.

Most of the others are not and should not be IT's concern per se — I'm thinking smartphones, tablets, and even so-called productivity tools, which are really job-specific tools. IT's job is to set the policies for access control, user authentication, information flow, and so forth — not to worry about the endpoint devices as long as they meet the policies.

Finally, there are the two special cases: public social media and social marketing management tools. Both can be considered departmental technologies that IT could manage or simply defer to an outsourcer or cloud provider, focusing IT's role on governance and data integration issues. In the 1990s, most large enterprises quashed the notion of departmental computing, as it led to duplication of infrastructure and breaks in information flow and process flow. But sometimes, organizations also blew up or absorbed truly departmental functions into bigger tools where they lost their focus.

Social media and social marketing are specialty activities, like HR management tools, accounting tools, and chemical analysis tools. They may hook into a common communications back end, get data from a common ERP or CRM system — what IT should own and manage — but the tools and processes related to the specialized social tasks belong in the business unit charged with social and marketing activities. These are the kinds of areas where IT and individuals have to ally, because both are needed for different aspects of the technology.

Consumerization is not a black-and-white phenomenon, and how to handle the technologies that empowered users requires more than a black-and-white solution.

*Galen Gruman is executive editor of InfoWorld for features, as well as its Mobile Edge blogger and Smart User blogger. Follow Galen's mobile musings on Twitter at MobileGalen and at Google+.*

IMPLEMENTATION

# How to mess up a BYOD rollout

Sometimes dumping mobile devices onto employees doesn't play out as planned

*By Galen Gruman*

THE GOOD NEWS IS THAT MORE AND MORE COMPANIES ARE LET-ting employees bring in their own smartphones and tablets, acknowledging the BYOD phenomenon. The bad news is that many are doing it badly and often regretting the results. It doesn't have to be that way, but an unhappy outcome seems to be the norm, especially at midsize companies, says Brandon Hampton, a director at Mobi Wireless Management, which provides a management service for mobile devices and carrier plans.

What shocked me was why so many customers are unhappy with the results.

## THE NAIVE MOTIVATION FOR BYOD

The typical experience, Hampton says, is that companies that decide to migrate a large portion of their users from corporate-provisioned smartphones to employee-owned units — in telco parlance, from corporate-liable to individual-liable — are unhappy that it takes 20 to 30 minutes per user to accomplish the transition, including device setup, message forwarding, and so on. Also, they normally can't reduce their telecom support staff when the transition is done even though they've doubled or tripled the number of users in the process.

My reaction: How can they not be happy that two to three times as many employees are now able to be productive when on the go, while maintaining the same support overhead? (Hampton reported that support calls drop from an average of 4.5 per user per year to 2.5 when employees use their own devices, and the nature of support changes from dealing with billing questions to dealing with corporate access questions.) I also thought, "How could they expect the transition to require no effort? Plus, don't they get it's a one-time investment in increased productivity?"

Hampton laughed at my naievete. The reason most companies — especially midsize ones — do a BYOD transition is not to increase productivity but to palm off telecom costs onto employees. Their goal is to reduce absolute cost; productivity and employee satisfaction are mere side effects. That of course is the problem: Their goals are naive, so what should be viewed as a positive outcome isn't. The problem is not that BYOD itself is negative, it's that many companies do it for the wrong reason and don't get what they wanted.

## POOR IMPLEMENTATION WORSENS NAIVE APPROACH TO BYOD

Some companies compound the (perceived) poor results by making other mistakes. One is to have employees expense their mobile bills, which costs about $25 per expense report to process (adding cost). Hampton suggests that companies pay a flat fee, perhaps in each paycheck, for mobile reimbursement for users whose mobile needs are moderate, and buy and manage the devices (and data plans) used by heavy users. In his experience, the flat-fee reimbursement is cheaper, especially if you base it on role and have just a few tiers of reimbursement amounts. If you tie it into your Active Directory monitoring, you can see which employees are accessing corporate resources via mobile and reimburse just those employees.

He recommends companies continue to provision devices to heavy users even if you let them choose which device to use, as is increasingly common. That way, you can usually get better coverage plans, especially for international travelers, when you bundle them as a package to a provider.

The other common mistake is not to have a mobile management strategy in place; whether a device belongs to the company or employee and whether or not the company pays for it, you manage access to your network and corporate resources using mobile device management (MDM) and other tools based on policies you should already have in place for internal access to corporate resources. It turns out that many companies don't do this, then get surprised when a departed employees' tablet ends up on eBay still containing corporate data.

Hampton notes that midsize companies struggle with these issues more than large ones because they typically have a "phone guy" rather than a team of people experienced with

the various areas, which include device management, security, policies, and carrier relations.

### THE "DUMP THE COSTS" STRATEGY MAY GAIN TRACTION, UNFORTUNATELY

Because the motivation at so many companies is to save money, but not increase employee productivity, Hampton has seen odd deployments. For example, one company charges its employees an annual fee for access to corporate resources from their personal devices. More surprising, employees are willing to pay this "convenience fee" to do work from their own devices.

Hampton has also seen companies purposely require the use of expense reports to claim stipends, knowing that many employees won't do the paperwork and the companies won't have to pay those stipends. Employee acceptance of such abusive actions only encourages the notion that BYOD means "shove the costs onto employees" rather than "let's figure out how to work better and smarter."

It's possible that "shove the costs onto employees" approach will only gain more acceptance. I've heard in the last year sev-

eral executives muse about having employees buy their own computers, selling it as an opportunity to use a computer of their own choosing. They saw that employees were willing to buy iPhones, iPads, and Androids — and that corporate security was not compromised in the process. Hampton has also heard such musings.

We've already seen companies stop paying for at-home phone lines and broadband, as employees willingly picked up the costs for their own convenience. Perhaps if this trend continues, we'll have to pay to use a desk at the office, like independent contractors such as hair stylists and real estate agents do.

I hope not. If a company's motivation is to shift costs to employees, BYOD and the consumerization-of-IT trend will fail to benefit that company in the medium to long term. The company will instead get employees used to standing apart from the organization, with the dire results that usually brings. You've been warned!

*Galen Gruman is executive editor of InfoWorld for features, as well as its Mobile Edge blogger and Smart User blogger, author of "Mac OS X Lion Bible," and lead author of "Exploring iPad 2 for Dummies."*

## Top 7 truths about consumerization of IT

*The phenomenon is only growing stronger. Here's what IT and business leaders need to know*



Users are no longer ignorant about technology; many are passionate and knowledgeable. Consumer-grade tools are ever more capable for business usage — and sometimes superior to traditional tools.

Your employees are using "consumer" mobile, cloud, social, and software tools, with both good and bad implications for productivity, responsiveness, governance, and security.

Here are the top 7 truths about the consumerization trend.

MANAGEMENT

# BYOD's uncharted legal waters

## There's no clear answer on the right legal approach for users and companies

*By Galen Gruman*

THE BYOD PHENOMENON QUICKLY MOVED FROM A "NOT IN MY business" option in 2010 to the de facto standard in 2011. BYOD also intermingles personal and professional usage, data, and ownership, creating uncharted territory for businesses and individuals alike as to who has rights over what, as well as to what are the best legal approaches to securing their respective interests.

Even in the BYOD world there remains the question of who should legally own the device, in addition to the questions of who owns the data consumed and created on it. The harsh truth is that there are no answers to these questions — the courts haven't ruled on them, and legislators haven't written laws to address them. The good news is that we're in a period of experimentation to see what works best; the bad news is that the resulting uncertainty and inconsistency make "doing the right thing" very difficult.

Until society figures out the rough answers itself, we're likely to stay in this situation, says Peter Vogel, an attorney at Gardere Wynne Sewell who specializes in and teaches technology- and communications-related law. (I recommend you read his blog on legal issues in IT regularly.) That's because the courts and the legislatures typically act when there is some consensus, not before.

Whether you're in IT, HR, legal, or a business unit, you're largely on your own about decisions on ownership of devices, data, and so forth. But you should be aware of clusters of approaches that could be starting points for what might fit your culture, risk tolerance, trust assessment, and regulatory context.

### THE POSSIBLE FORMS OF DEVICE OWNERSHIP

Although the era of the company-owned and company-provisioned mobile device seems to be coming to a close, there's still an ownership issue — or at least a permissions issue — to be addressed. These issues apply to more than just mobile devices, though it's a rare company that seems to think them through for employees' home PCs and the like, which

face the same fundamental issues.

Organizations in government, health care, and defense especially face the legal question of who actually needs to own the device, though the concern isn't exclusive to them. There's no clear answer to that question as yet, but the underlying issue concerns when ownership is necessary to gain management control. But more conservative organizations often decide they need legal ownership of the device.

The result has been three different approaches to handling ownership, in order of popularity:

**Shared management.** The organization's contractor and employment policies boil down to "if you access business resources from a personal device, you give us the right to manage, lock, and even wipe that device, even if you end up losing personal data and apps as a result." This is often codified with a written agreement that spells out management expectations for both parties.

**Corporate ownership and provisioning.** The organization buys and owns the device, even if it allows nonbusiness use on it. Employees who don't like the phone service on such devices (they may not get free minutes when calling family members and friends) are free to carry a personal device as well that has no corporate access.

**Legal transfer.** The organization buys the device from the user. In some cases, that ownership is permanent — a surefire way to dissuade employees from participating. In other cases, the organization buys the device for a token amount (say, a dollar) and gives the user the right to use it for personal purposes, then commits to selling it back for the same price when the employee leaves the organization. That's more likely to gain user acceptance than a one-way purchase.

I've heard from several organizations recently that took the legal-transfer approach but are now rethinking it and getting more comfortable with shared ownership. The number of companies insisting on corporate ownership is shrinking, except in industries where the devices are custom, such as the signature pads used by UPS and FedEx drivers.

Vogel says that none of these approaches is more right or wrong from a legal point of view — yet. But if you want to

ensure access to all communications and data on the devices (including PCs), you need to own them, for reasons explained later in this post.

If you have European employees, you need to be aware of an additional factor, notes SAP CIO Oliver Bussmann, who supports 12,500 iPads in a mix of corporate- and employee-provisioned devices. That factor is European privacy rights, which lets employees opt out unilaterally from their agreement of giving employers access to their personal information, even incidentally, in a context such as BYOD. There's no easy way to address this issue; the employees often bring enough benefit to the company with such access that cutting them off would hurt too much.

## THE UNCERTAIN OWNERSHIP OF DATA

It used to be that in the United States you could reasonably assume that personal information communicated through cellphones and other such devices were considered private to the employee, based on various court cases and a set of laws called the Stored Communications Act. The key to that privacy was that the data was stored by a third party (a telco or Internet service provider), not by the company, which would have access to rights to whatever it stored, such as on its email servers. Essentially, the Stored Communications Act extended Fourth Amendment protections of a person and his or her property to that person's electronic data even when stored on "neutral" property (that is, a telco's or ISP's servers).

But last year, the Supreme Court upended that assumption in a ruling that said employers had the right to access all communications on corporate-issued devices, regardless of where it was stored. Vogel says that this unanimous ruling essentially sidelined the Stored Communications Act, which had originally been designed to address subpoenas of chat boards and the like, not mixed-use devices such as corporate cellphones.

The court explicitly said that right to access applied to corporate-owned devices. That could suggest the justices intended that employee-owned devices don't fall under companies' information access rights, Vogel says — or it could simply mean the justices didn't think through their ruling in a BYOD context, which at the time was still emerging, and at some point they'll fix what was an inadvertent limitation.

As a result, strictly speaking, employees have no privacy rights for what's transmitted on company equipment, but employers don't necessarily have access rights to what's transmitted on employees' own devices, such as smartphones,

tablets, and home PCs. Also unclear are the rights for information that moves between personal and corporate devices, such as between one employee who uses her own Android and an employee who uses the corporate-issued iPhone.

This confusion extends to trade secrets and other confidential data, Vogel notes, as well as to e-discovery. When employees store company data on their personal devices, that could invalidate the trade secrets, as they've left the employer's control. Given that email clients such as Outlook and Apple Mail store local copies (again, on smartphones, tablets, and home PCs) of server-based email, theoretically many companies' trade secrets are no longer secret.

This automatic local storage can also cause issues in e-discovery, both in terms of whether personal devices are subject to such discovery and what happens when normally purged information still exists as a copy on an individual's personal device. An employee could keep local copies in hopes of later blackmailing a company, for example, or more innocently have part of a communications thread that could be seen as damaging only because the rest of the context was purged as part of normal data-cleansing operations.

Until something changes in the law or in future court rulings, owning all the equipment an employee uses does give a business the most control over its data and communication. Of course, that contradicts the trend to let people use their home PCs and personal devices, which many businesses like for the cost savings and lower accounting and asset-management overhead.

The real question: What's that control worth to your business?

The bottom line is that the laws and court cases haven't caught up to the intermingled world of consumerization, where information flows through both personal devices and corporate devices, where data travels through a mix of corporate, personal, and third-party networks and services (think "cloud"), and where it is stored in a mix of corporate, personal, and third-party locations (think Gmail, Salesforce.com, Amazon Web Services, iCloud, Office 365, local mail clients, home PCs, and so on).

The good news is that whatever you're doing is probably not wrong, legally speaking. But the bad news is that it may not be right, either.

*Galen Gruman is executive editor of InfoWorld for features, as well as its Mobile Edge blogger and Smart User blogger, author of "Mac OS X Lion Bible," and lead author of "Exploring iPad 2 for Dummies." Follow Galen's mobile musings on Twitter at MobileGalen and at Google+.*

MANAGEMENT

# Why IT and business clash

## IT's unique culture frequently differs from that of the rest of the business

*By Bob Lewis*

WHEN IT AND BUSINESS STAFF CLASH, THINGS CAN GET UGLY quick. Everyone has experienced some measure of tension across the business/IT divide. But is that tension a simple clash of personalities — or is it a clash of cultures? Solve the wrong problem, and tensions are likely to escalate.

At many organizations, this environment of conflict between business and IT is commonplace. It hinders daily operations and interferes with ongoing projects. Worse, it can prevent IT from evolving to meet the expectations of next-generation IT.

As a result, fixing this tension should be a high priority for everyone on both sides of the divide. And the first step in fixing a contentious business/IT relationship is an accurate diagnosis. If you get that wrong, if you don't fully understand why IT clashes with the rest of the business, your solution has virtually no chance of working.

### NEXT-GENERATION IT

As a reminder, next-generation IT embraces three core principles (he asserted with his usual and abundant humility):

1. IT is the steward of the company's information resources, not the owner

2. IT empowers end-users to be innovators by opening new technological doors for them as motivated by end-user choice

3. IT is strategic in supporting "single-actor business practices" — a significant tactical shift from years of paying attention only to core processes

To play that role, IT needs a positive, healthy, and properly defined relationship with the rest of the business. The question is how to make that happen.

### PERSONALITY VS. CULTURE

Communication between IT professionals and business professionals is frequently ineffective, and this is a problem that has to be rectified if the business/IT relationship is to be placed on a solid footing.

This lack of effective communication is a root cause of dysfunctional business/IT relationships, not the root cause.

Were you to ask all 16 of us where we disagree, however, you'd probably get 16 different answers. This is, after all, a work in progress and we have more progress yet to make than progress yet achieved.

Here's my take on the nub of it: Some in the conversation believe the core issue is that IT professionals have a distinct personality type. We're geeks, geeks have a different way of thinking than the non-geeks who inhabit the rest of the enterprise, and it's the difference in how we think that's the core issue.

Assuming there is a distinct geek personality type, what is it? As a quick short-hand, figure it's everything pop-psych usually associates with left-brain thinking: linear, logical, analytical, and so on. My own view is that the geekiness that characterizes IT is due less to personality type than to IT professionals being embedded in a distinct, "geek" culture.

### THE MATHEMATICS OF PERSONALTY CLASHING

No matter how strongly anyone thinks that "geek" is a personality type, nobody would claim that everyone in IT is a geek, or that everyone outside IT isn't a geek. For that matter, it's doubtful anyone would consider geekiness to be an all-or-none proposition: If geekiness is a personality type, it's a continuum, with uber-nerds on one end of the scale and performance artists on the other.

Let's imagine, for the sake of argument, that two out of every three IT professionals have a lot of geek factor in their personalities, while only one out of every four non-IT employees does — quite a strong correlation between personality type and profession; the numbers aren't likely to be more extreme than this.

Given these numbers, two-thirds times three-quarters ... half ... of all interactions between IT and non-IT employees will be between IT geeks and non-IT non-geeks.

That's enough to present a challenge, but not so overwhelm-

ing as to characterize the whole business/IT relationship.

## GEEK CULTURE: THE GREATER ISSUE

Compare this to the cultural diagnosis.

Culture has been defined by lots of different people in lots of different ways. My own consulting company borrowed its definition from a branch of anthropology called ethnoscience, which defines culture as "the learned behavior people exhibit in response to their environment."

An interesting bit about "their environment" is that in a business setting, most of the environment each employee works in is the behavior of the other employees they work with. It's a self-reinforcing loop, which means that unlike personality, which varies a lot from one employee to the next, culture is shared. Those who participate in it acculturate ... they converge in how they respond to different situations.

So while even with some fairly extreme assumptions, personality-type-driven clashes are likely to be the cause of conflict in no more than 50 percent of all IT/non-IT interactions, a clash of cultures is built into the fabric of things.

And make no mistake: IT does have a distinct culture. It has to, because in order to succeed in the work, all IT professionals have to approach their work with a certain mindset that's different from how employees who plow the fields of marketing, sales, manufacturing, human resources, and even accounting and finance think about their responsibilities.

## DEALING WITH CULTURE CLASH

As do employees who work together anywhere, those of us who work IT develop a shared vocabulary, a set of largely unconscious shared assumptions, and shared patterns of thinking. These shared cultural traits streamline and simplify our communication. A common culture makes IT more effective.

Regrettably, they also lead to IT professionals thinking of everyone in IT as "us" and everyone else in the company to be

"them." It's a dangerous state of affairs, as dividing the world into us and them is how tribalism happens — how we come to consider our self-identified group to be the source of all that's right and good in the world, while all the others are shifty, dangerous, ugly, and (lucky for us) incompetent, too.

"We" can't trust "them," and the proof is that when we try to explain our position on an issue, they just don't get it, and when they try to explain their position on an issue, they're utterly incoherent, or else they just lie to us.

Oh, and by the way: It's worse — within IT we have distinct subcultures that clash as well, as anyone knows who has heard Unix and Windows sysadmins go at it on an engineering issue.

Humans are intrinsically tribal creatures. Want evidence? Over and over again, when studying languages, it turns out the word people use to refer to themselves is "the people." Everyone else in the world? They aren't included.

So you aren't going to solve the inevitable clash of cultures by lecturing on the evils of tribalism. All that will do is reinforce the view held by everyone in your tribe that they're just fine. The problem, your fellow MoTs (Members of the Tribe) will conclude, is that "they" are so tribal, unlike us.

No matter where you sit, inside or outside IT, and no matter what your level in the organizational hierarchy, you have a role to play in solving this.

You might think the solution is tolerance, but it isn't. Tolerance just won't cut it, because all it requires is that you learn to put up with those idiots. That's what "tolerate" means.

No, what's needed is deeper and more difficult than tolerance. What's needed is respect — the recognition that different doesn't have to mean better or worse. It can mean each tribe has something to learn from the others.

*Bob Lewis is president of IT Catalysts, Inc., an independent consultancy specializing in IT organizational effectiveness and business integration. He's the author of Leading IT: (Still) the Toughest Job in the World, nine other books, and more than 800 articles on managing information technology organizations. Bob Lewis writes the Advice Line blog for InfoWorld.*