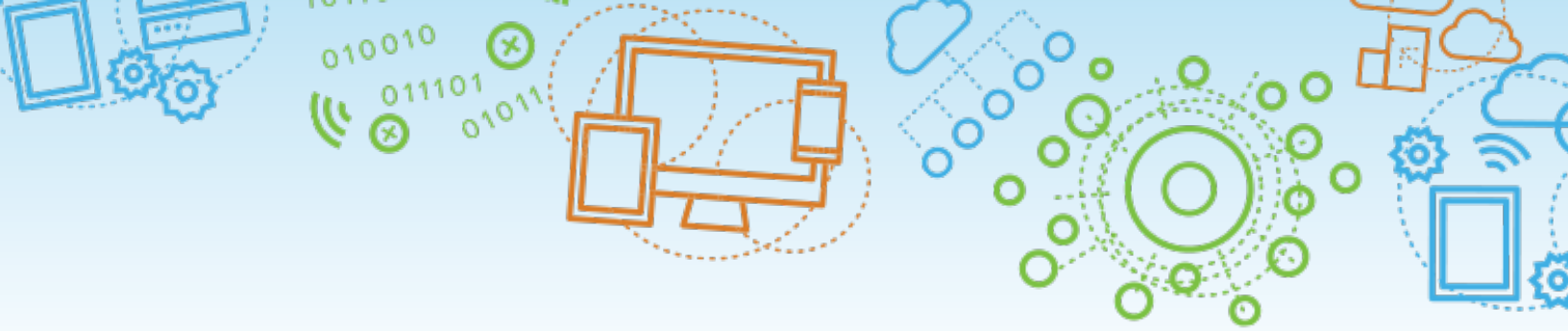

The Apple-ization of the Enterprise: Understanding IT's New World

Written by Phil Simon for Code 42's "Apple-ization of the Enterprise" Educational Initiative

EXECUTIVE SUMMARY

Today's "always-on" knowledge workers demand and will settle for nothing less than an Apple-like experience from their devices and applications. But when Apple fanboys rush to buy the company's latest creations for use at home and at the office, many CIOs and IT managers cringe. They wonder how—given this rapidly changing, technology-laden world—they can support even more devices, apps and networks; properly protect enterprise data; and maintain compliance with existing/emerging regulations.

These are legitimate concerns from executives who have seen firsthand the perils of emerging, consumer-grade technologies introduced into their IT environments. One cannot fault CXOs for worrying about the consumerization of IT, not to mention the next-gen "Apple-ization of the Enterprise."

So, it's fair for a senior leader to ask, "How can IT make things easier for end users while also concurrently meeting the security, compliance and privacy needs of the organization?"

It's a big question today, and the stakes are particularly high.

Fortunately, however, IT departments are in luck. A new set of tools and applications can help them keep just about all of their constituents happy: everyday employees, senior management, regulatory bodies, auditors, etc. Rather than fighting this inexorable trend, IT departments can embrace "Apple-ization of the Enterprise" and reap massive rewards in the process. This white paper describes how.

We've become accustomed to self-service as consumers, and we don't turn off that mind-set once we head to work.

Background

Consumer markets for mobile devices and software continue to collectively drive technology and applications, tremendously impacting how work gets done. At the same time, employees have become fundamentally impatient, increasingly tech-savvy and seemingly always tethered to their devices. As a result, their expectations of enterprise technology have grown exponentially.

Today, software has to do more than just work; employees have to find it intuitive and enjoyable. Constantly connected knowledge workers (especially Millennials) want an Apple-like experience from all their devices and applications, and many will leave if they don't get it.

While this may scare enterprise IT departments, there's a flip side to this coin: thanks to tablets, smartphones and social networks, employees can be incredibly productive while away from the office. As History Professor Melvin Kranzberg once famously wrote, "Technology is neither good nor bad; nor is it neutral."

Without question, the Apple-ization of the Enterprise offers many benefits for both employees and the enterprise: convenience, efficiency and productivity.

Consequently, an increasing number of progressive enterprises have embraced today's new (*read: Apple-centric*) reality. More companies are **buying Macs, iPads and other Apple products in bulk** because making employees happy by supporting user-friendly devices and applications is key. Management also realizes, however, that blindly supporting a swath of untested software and hardware in the enterprise is not the answer.

So IT faces a tricky dilemma: how to control and secure the IT environment while *concurrently* keeping impatient, multi-device-holding employees happy and productive? There's no simple answer to that question. On one hand, popular productivity apps and devices certainly benefit consumers. On the other, many of these apps and devices contravene enterprise needs, particularly those around security, performance, compliance and scalability.

As a result, the bar has been raised for enterprise IT teams and IT professionals. Today, IT's role involves much more than just ensuring employee productivity, data protection and enterprise security; it's also about providing an optimal user *experience*.

Today, IT needs to concurrently serve two masters: the needs of the enterprise and the desires of the employees. Successfully navigating this tension is not easy, but failure to do so will cause a raft of organizational problems.

Apple-ization Challenges for the Enterprise

Forward-thinking organizations wanting to welcome Apple-ization of the Enterprise must be reassured their IT teams will retain confident control, management and secure access of corporate data.

This white paper discusses five of the most common challenges faced by progressive organizations when

Five Common Challenges for Embracing Apple-ization:

Endpoint backup and restore

Client management

Enterprise mobility management

Malware and device security threats

Working with the business

embracing Apple-ization of the Enterprise, with advice for how to jumpstart each initiative:

- Endpoint backup and restore
- Client management
- Enterprise mobility management
- Malware and device security threats
- Working with the business

Let's discuss each.

Back Up and Restore Data on Laptops/Desktops

You've probably seen this drama before: your hard drive crashes, and you haven't backed up your data. Well, at least you're not alone. According to a Computer Troubleshooters 2012 report, over half of all critical corporate data resides on unprotected PC desktops and laptops, even though one in 25 notebook computers is stolen, broken or destroyed each year. In a word, *wow*.

This begs the critical question: how can IT easily secure enterprise data residing on employee devices in a continuous and unobtrusive way? Employees don't want IT over their shoulders while they're working, and software programs might not be the answer. Some existing backup programs and services effectively freeze devices, creating mandatory "backup breaks." And for their part, IT professionals would prefer not to spend their time trying to restore users' data.

Arek Sokol, senior Mac engineer for Genentech/Roche, is reaping the benefits from the biotech leader's public cloud deployment of CrashPlan for enterprise endpoint backup. "Eliminating onsite equipment saves on everything from power to admin time," Sokol explained. "We're pretty much a virtual shop anyway. Most of the tools our employees use are in the cloud, and CrashPlan helps us make sure everyone is backed up, wherever they are."

The company's backup strategy is critical to its overall global consumerization strategy. "CrashPlan plays an important role in our goal of being an innovative, 100 percent virtual global company," continued Sokol. "It's one of the core services we'll trust and rely on in the future."

SIMON SAYS

Bottom line: it's imperative IT gives employees a way to easily access and quickly restore their data. At the same time, Apple-ization environments demand cross-platform support in order to ease management and support burdens. Solutions like Code 42's CrashPlan can be invaluable in such circumstances. For example, the CrashPlan mobile app allows employees to access any CrashPlan-protected file at any time, from anywhere, from any device. So IT keeps the data safe and sound (locked down with device-side encryption keys), and users can get to their documents whenever necessary—a true Apple-ization win-win. The solution's support of all leading platforms means IT can support all users from a single solution and single management console.

Client Management

This isn't 1999; no longer does the PC necessarily rule the enterprise. As Macs and iOS devices continue to make inroads in the enterprise, companies seek new tools to support MacBooks, iPads, iPhones and other devices. As a result, IT administrators now face a new set of challenges: IT tasks now include endpoint

deployment, routine software updates, new software distribution and rapid tech support—*across a number of devices and applications*.

For Tim Winningham, systems manager for the math department at The Ohio State University, effective client management is at IT's core in his higher ed setting. "With BYOD taking hold and new machines entering our environment daily, we were given a mandate to track all of our non-capitalized assets, and we had to do it right away," Winningham recalled. "We needed to have a record for every computer, monitor, printer and external hard drive."

JAMF Software's Casper Suite featuring "integrated inventory management" provided the answer. Winningham described the simple process: "Slap a sticker on it and add it. Even with non-controlled items, the database was already in place for us." Automating the inventory/asset tracking process with JAMF's powerful client management technology immediately fit the need and set the groundwork for OSU's campus-wide support for IT consumerization and BYOD.

SIMON SAYS

In general, IT typically provides varied support experiences based on types of devices, but that doesn't make sense to the end user. Put simply— no matter which device they're using, end users want to reach content, communicate and get IT support. And, they don't want to be disrupted by hardware and software monitoring services.

Client management needs to support those needs of end users while enforcing corporate policies, maintaining organization standards and meeting compliance requirements for all devices on the network. Management tools like Casper Suite can save IT tons of time by effectively, quietly managing clients while providing a friendly experience for end users.

Enterprise Mobility Management (EMM)

Think back for a moment to a few years ago. iPhones and Android smartphones began invading the enterprise *en masse*. BYOD terrified many CIOs. The fear was that all of these devices were completely unmanageable. Soon enough, though, solutions to manage them began to emerge, and organizations started working with application programming interfaces (APIs) to make devices more secure.

And it's not slowing down anytime soon. According to the ***Financial Times***, the size of the smartphone market has surpassed the PC market, turning mobile device management (MDM) into a critical topic for enterprises.

As Nick Heath wrote on **TechRepublic**, "Since the iPhone launched in 2007, Apple has been slowly increasing security of iOS devices: adding 256-bit, hardware-based encryption for data stored on the device, widespread VPN support and limiting access that each app has to files and hardware resources on the phone. That's in addition to its screening of all software on the app store and centralized control provided by third-party mobile device management software."

So the question of whether tablets and non-Blackberry smartphones can be secured and managed has been put to bed. Now the debate changes to *how*

Get started with an enterprise mobility management strategy, including:

Mobile asset inventory

Mobile device provisioning

Mobile software distribution

Mobile security management

Mobile data protection

Monitoring and help desk support

organizations should approach MDM. Mobile information management (MIM) and mobile application management (MAM) are evolving as we speak. Enterprise mobility management (EMM – the marriage of MDM, MIM and MAM) means that corporate data and apps can be secured and managed—*even if the device is not*. Each "management" area secures different levels of the mobile spectrum, from physical devices to their apps and data; combined, they are all part of a comprehensive mobile security strategy for the enterprise.

SIMON SAYS

In the Apple-ized enterprise, IT should embrace EMM. It's not a fad, and it's not as hard as you might think. TechTarget provides a valuable checklist for getting started with an enterprise mobility management strategy, including:

- Mobile asset inventory
- Mobile device provisioning
- Mobile software distribution
- Mobile security management
- Mobile data protection
- Monitoring and help desk support

Malware Threats

In an era of BYOD, protecting laptops, desktops and mobile devices has never been more personal. It's incumbent upon IT to provide employees with the peace of mind they need to be productive at work. Protecting the end user is paramount, and, contrary to popular myth, Apple products get viruses, too. As a result, enterprise IT departments must effectively embrace a more "personal" approach to securing devices. They must be prepared to support all common platforms, like Windows, Mac, Linux, iOS and Android.

As a critical first step, IT needs to reduce the attack surface and develop a layered security strategy that provides better protection.

SIMON SAYS

Lucky for us, malware/anti-virus leader Sophos publishes loads of helpful content in its "Security Trend Report," featuring everything from mobile security toolkits to password tips and ways to stay ahead of "hacktivism."

Device protection is critical to a successful Apple-ization strategy in order to ensure laptops, desktops, phones and tablets do not breach corporate security policies. To get started, build out plans to:

- Enforce your security policies for corporate and employee-owned devices
- Block access to company resources for non-compliant devices
- Give your users the apps they need to do their jobs, then block others
- Provide secure mobile access to company resources
- Prohibit personal devices from slowing down your business

Working with the Business

I can't stress enough the human side of technology. Each gadget, app, program and database does not exist in a vacuum. As I wrote in *The Age of the Platform* and *The New Small*, the most powerful technologies don't guarantee anything.

If people can't communicate effectively and work well together, the organization will suffer.

Today's technical and non-technical employees do not work in silos. They need to work *together* on key projects

IT and end users need to break through the circle of mistrust and avoidance in order to build effective, collaborative working relationships.

and at key times. Lamentably, however, they find themselves on vastly different pages. General frustration caused by the other is far too common. (The reasons for this are beyond the scope of this paper. Suffice it to say for now that often geeks and non-geeks see the world in fundamentally different ways.) Each group has different assumptions about how the world works and, more important, how it *should* work. It's not uncommon for meetings and conversations to result in impatience, frustration and miscommunication.

So writes Paul Glen, co-author of *How to Manage and Lead the People Who Deliver Technology*: "For IT to become more influential, it must learn to empathize. It must consider the thoughts and experiences of those it wants to influence. And then it will have to decide whether it wants to be powerful or influential. Ultimately, IT professionals need to ask themselves, 'Are we willing to put in the effort it will take to change people's minds?'"

SIMON SAYS

For any enterprise to succeed, IT and end users need to break through the cycle of mistrust and avoidance in order to build effective, collaborative working relationships. And perhaps the Apple-ization strategy is a good place to start. After all, Apple-ization encompasses both the consumerization of IT and BYOD—and the IT/end-user relationship is at the heart of both trends.

Make it a priority to empathize with business users and understand their worldview. Leading Geeks, an organization dedicated to transforming how technology and the people who deliver it contribute to their companies, can provide insight into how enterprises can embrace Apple-ization by bridging the fundamental differences between IT pros and non-technical users.

Conclusion

Today's employees carry with them more powerful devices than the best computers of 1998. And, with social networks and the Internet, they can do things that are both amazing (good and bad) and irrespective of any enterprise's official policies.

In short, most workplaces are increasingly becoming Apple-ized, whether CIOs like it or not. Against this new backdrop, IT departments face both significant challenges and opportunities. Sure, something like BYOD saves organizations from the potentially substantial cost of provisioning devices, training employees on their use and the like. But foolish is the CIO, however, who doesn't recognize the fleas that come with this dog. Left unfettered, employees who use unregulated devices and apps saddled with questionable or nonexistent privacy and security safeguards can cause a great deal of harm. Compliance, privacy and security issues are just a few of the headaches facing IT departments in this new employee-driven Apple-ization of the Enterprise era. Chaotic or *laissez faire* environments only serve to exacerbate these issues and increase the risk of fines, lawsuits and breaches.

Fortunately for IT, many tools exist that allow organizations to have the best of both worlds. That is, they can reap the benefits of Apple-ized employees while minimizing the costs. A seemingly insurmountable task, prioritization according to your organization's specific

needs and a phased implementation approach have helped early adopters welcome Apple-ization into their enterprises while confidently protecting corporate data. You can, too.

Additional Apple-ization Resources

Visit **www.enterpriseappleization.com** for more from Code 42's Apple-ization of the Enterprise initiative—an ongoing forum and resource for IT teams struggling to securely and confidently address this movement while also properly protecting enterprise data. The site is intended to be a one-stop shop for enterprise IT teams seeking relevant information, tools, techniques and checklists related to Apple-ization. Find more relevant info at:

- Initiative: Apple-ization of the Enterprise
- Webinar: IT's New World: Understanding Today's Empowered Employee
- White paper: Apple-ization of the Enterprise
- White paper: Enterprise Backup in the Age of IT Consumerization

About the Author

Phil Simon is a sought-after speaker and the author of five management books, most recently *Too Big To Ignore: The Business Case for Big Data.*

A recognized technology expert, he consults companies on how to optimize their use of technology. His contributions have been featured on NBC, CNBC, *Inc. Magazine*, *BusinessWeek*, *The Huffington Post, The Globe and Mail, Fast Company, The New York Times*, ReadWriteWeb, and many other media outlets.

About Code 42 Software

Code 42 Software has been developing software to protect the world's data since 2001. Code 42's CrashPlan enterprise endpoint backup solution is used by thousands of companies around the world to safeguard data housed on laptops and desktops.

The company also offers industry-leading backup software for homes and small businesses. All products offer multi-destination, cross-platform backup to public, private and hybrid clouds.