Introduction

Many organizations that were early adopters for BYOD (Bring Your Own Device) have come to the realization that a successful BYOD program isn’t as easy as installing hardware and software or executing a plan, no matter how carefully that plan was put together. BYOD 1.0 may not have met expectations, but there are ways to optimize your policies and procedures so they support new technology, increase ROI and satisfaction. In this case, “new technology” means next-generation portable devices that employees want to use, but it also means new evolutions of infrastructure components like cloud servers, storage devices, security measures and network infrastructure.

BYOD in a Post-PC World

BYOD policies allow employees to bring personal portable devices such as laptops, tablets, and smart phones into the workplace and connect them to a network that allows access to corporate applications and data. This trend is exciting for employees who see increased flexibility and productivity, but it complicates things for IT staff in charge of keeping corporate information available, secure and compliant. Either way, BYOD is here to stay. Industry leaders and analysts agree we are living in a “post-PC world”¹. Post-PC devices are devices with no keyboard or mouse, so they are extremely convenient and portable. These devices are so widely consumerized that most employees are already using more than one kind in their personal lives. Also, the majority of the next generation of employees is more accustomed to post-PC devices than current employees. In fact, a 2012 report revealed that 77% of U.S. adults own a laptop, 44% of adults own a smartphone² and 22% of adults use a tablet³. Thirteen percent of all adults in the U.S. own all three.

³ [http://www.engadget.com/2012/10/02/pew-research-center-tablet-ownership-report/]
Considering the level of functionality and convenience consumers are accustomed to in their personal lives, it’s no wonder they are quickly frustrated with dated corporate technology, cumbersome operational and security policies, carrying duplicate devices or adjusting to a one-size-fits-all approach at work. After all, one of the main purposes of technology is to consolidate and streamline. Nobody wants to carry a phone and a laptop, and certainly nobody wants to carry two phones and two laptops. Most key employees, mobile employees and executives flat out refuse to carry duplicate devices or any corporate-issued device that is inferior to their personal device.

Organizations that employ “millennial” employees find they are dealing with a generation that has never known life or work without integrated technology. Many of these organizations backed down from their original no-personal-device policies when they realized it was happening whether they liked it or not - and that if they stood firm they’d have to deal with unhappy employees, lost productivity, lost profit and brand damage. Additionally, anti-BYOD policies can cause organizations to lose competitive points in the war for talent. It’s estimated that 74% of organizations allow some kind of BYOD\(^1\) so it appears that many businesses that once resisted BYOD technology are now enjoying the benefits. Recently Dell revealed its Global BYOD Survey results and determined “…companies that embrace a user-focused approach to BYOD may reap the biggest rewards, while those slow to support BYOD or constrained by a device-centric approach may deal with greater challenges, including the risk of being left behind from a competitive standpoint\(^2\).”

---


The biggest mistake an organization can make is to assume they can solve the problem simply by prohibiting personal devices regardless of policy - except now the use isn’t monitored, isn’t controlled and is usually below the radar.

Prohibition Doesn’t Work

For IT administrators, it’s not as straightforward as giving people permission to use personal devices at work. The desktop has always been the administrator’s domain, a place where they provide a highly controlled version of what they believe is right for the user. It’s a tough job because IT availability and security are critical, high visibility responsibilities, but most administrators lack sufficient authority, time and budget to monitor and enforce total BYOD prohibition. At the same time if data is lost, leaked or not available the bull’s-eye for blame is squarely on IT, fair or not. Unless the nature of their industry is totally unsuited for BYOD, IT administrators must find a way to make BYOD work with the technology and tools at hand.

Security concerns about BYOD are valid and must be addressed, but the biggest mistake an organization can make is to assume they can solve the problem simply by prohibiting personal devices. History shows that employees end up using their own devices regardless of policy – except now the use isn’t monitored, isn’t controlled and is usually below the radar.

BYOD ultimately is good for most organizations because it gives users the flexibility and choices they want while enabling seamless mobility for employees and a responsive business across a spectrum of devices. Implementation doesn’t have to be a white-knuckle experience. It simply must be deployed thoughtfully. After all, a predictable deployment gives the power back to the business.

Why BYOD Hasn’t Met Expectations.. So Far

When it comes to BYOD, IT administrators have a certain measure of fear, uncertainty and doubt and reactions run the gamut from completely committed to completely terrified. On one hand, most administrators want to embrace the BYOD trend because of increasing pressure from key employees and upper echelon executives (and, in some cases administrators were the first to bring their own devices). On the other hand, BYOD implementation seems expensive, and administrators may not be sure what BYOD means to their current security and compliance infrastructure. As they try to get a handle on what BYOD means to all parts of the organization, administrators and executives are wading through a labyrinth of questions:

- **Ownership** - Who’s going to own the device – the company or the user? Who owns the license?

BYOD Policies

<table>
<thead>
<tr>
<th>Prohibit BYOD</th>
<th>Allow some kind of BYOD</th>
</tr>
</thead>
<tbody>
<tr>
<td>26%</td>
<td>74%</td>
</tr>
</tbody>
</table>
• **Support** - If employees can buy whatever they want, who’s going to support all those different devices?

• **Security** - Who’s going to make it secure?

• **Accountability** - Who’s accountable if it’s lost, misused or stolen?

• **Compliance** - How will BYOD affect regulations and SLAs?

• **Application consistency** - Will users be permitted to download whatever applications they want? Should we consider Virtualized Workspaces for application consistency?

• **Unauthorized downloads** - How will we handle downloads? Will unauthorized downloads bring a plague of viruses?

• **Performance** - Will multi-media streaming slow down network performance?

• **Impact** - Will BYOD impact the company culture? Will employees go mobile and disappear? Will they be more disconnected?

• **Procedures** - Will we have to write new policies and procedures?

• **Intangible ROI** - What does the organization get out of BYOD? If employees are happier, is that enough?
• **Consistent Experience** - Can we provide a consistent user experience where it’s important?

• **Access** - What happens if a mobile employee is relying on their device but loses access to WiFi?

• **Status Quo** - Will BYOD disrupt the IT status quo?

• **Consumerization** – Who owns the hardware and repayment schedules?

For organizations that spent the better part of the last two years fighting BYOD, waiting for more mature technology or the perfect solution, it’s become clear that waiting isn’t going to make the situation better or easier. IT savvy employees will use their own devices at work, whether you want them to or not, and they’ll help less technology savvy employees do the same.

Like all technology, BYOD will evolve hand-in-glove with the technology around it. There will also be new benefits and new risk with every evolution and iteration; the prevailing wisdom is not to wait for BYOD 2.0. It’s essential to adopt a BYOD model and BYOD infrastructure components that support the existing desktop now rather than be left behind. Of course, BYOD won’t be right for every industry or business, but it certainly is worth the effort to investigate whether or not the current BYOD is good enough. If it’s not, you’ll be able to communicate the reasons to employees.

If you see signs of BYOD possibility, even though you may not be able to address all of the challenges, you will be able to address some of the challenges and your employees will note the progress (and enjoy whatever benefit you are able to provide). In other words, doing nothing is worse than doing something, even if the “something” is letting the workforce know you’ve thoroughly investigated the risks vs. benefits and BYOD isn’t right for the organization.

Rest assured, even though BYOD technology may not be mature enough for some organizations now, it will catch up. Organizations who need to wait will require new technology, better-integrated solutions or offline ability to access applications and data directly from users’ personal devices. Expect licensing to be updated to reflect the new paradigm. It’s just a matter of time, but wait at your own risk.
Benefits of BYOD

A successful BYOD program may be more involved than previously imagined, but investing the time and effort to ask the right questions and talk to an experienced consultant can help organizations of all sizes reap the rewards BYOD can offer. While there is some perception that the only benefit of BYOD is increased employee satisfaction (or at least less complaining), in most cases there is a solid business case for implementing a BYOD policy.

- **Mobility** - BYOD enables more flexible working hours for employees. Because most people take work home with them and require access to documents and corporate data when traveling, BYOD gives them a way to manage their workload in the different segments of their life.

- **Productivity** - If an employee's work device is the same as their personal device, they're more reachable when needed. They're also more likely to use moments of downtime – time spent waiting in lines or on public transportation, for example, to check in with work. These moments add up – waiting on an easy response from one person can hold up the entire team.
Creativity - Portable devices come with a lot more creative tools than PCs. Creative apps and functionality can boost creativity – and creative contribution to corporate efforts such as social media.

Retention - Employees expect BYOD-friendly employers. In the war for talent, those who allow BYOD will have a competitive advantage.

Savings - Organizations that allow workers to bring their own devices to work eliminate the need to purchase equipment. Fifty percent of companies with BYOD policies require employees buy their own devices – and most don’t mind1.

Agility - A BYOD culture allows people to share ideas at any time from anywhere. Again, those quick check-ins add up, allow people to be accessible while still enjoying their personal life.

Teamwork - When employees are able to work with their team from anywhere, they’re more likely to blur the lines between work life and personal life. While this makes the company sound as if it’s ready to wring more work time out of employees, people are usually happier when they can keep collaboration moving no matter where they are. Keep in mind that collaboration may require a change in technology or transition to Cloud services in order to support multiple devices and OS’s.

Improved Security - In many cases, analyzing and shoring up the technology and processes needed to enable BYOD can actually improve the security.

Optimizing BYOD for New Technology

If you’re starting to warm up to the idea of BYOD you may be wondering where to begin. Start by asking the fundamental questions, addressing security and analyzing the benefits in order to build a business case. Finally, map out a strategy. Like any implementation, planning, communication and controlled execution are the keys to success.

12 First Steps

1. Evaluate your user base by segmenting your workforce into use cases. Consider the security and regulatory implications of use cases, particularly for access and sensitive data. Consider how each segment consumes IT – is BYOD appropriate for all users? Some? None?

2. Identify risks that BYOD introduces into the IT infrastructure

3. Correlate risks with regulations

4. Establish policies for device connection

1 www.good.com/resources/Good_Data_BYOD_2011.pdf
5. Determine how you will manage applications
6. Establish a process for audits and reporting
7. Determine necessary level of network and data security
8. Determine how to handle retired devices
9. Determine how you will grant and revoke access
10. Consider the performance impact on your existing network
11. Consider the impact on storage
12. Determine how to evaluate new technologies and how you will evolve

**Fear, Uncertainty and Doubt Addressed**

**Ownership:** Who owns the device?

Today the allocation of employee vs. corporate-owned devices is about 50/50. Bulk corporate discounts from carriers and vendors make it attractive for organizations to include mobile devices in their benefits packages. When employees can choose their own devices, the corporation doesn’t have to try to please everyone and employees are free to choose the device that suits them, within corporate guidelines. Remember that surveys show that even when employees have to buy their own devices – they’re still happy.
Support: Who supports the device?

IT administrators can’t be expected to be experts on every mobile device that comes along, so it becomes a joint effort to support BYOD technology. One strategy that has been successful is to form device user groups in corporate intranets where users with the same device can ask each other questions and share knowledge.

Security: How will I keep data secure?

In reality, security is the foremost roadblock to adopting a BYOD model. However, security only becomes a serious concern when you don’t think about security implications during BYOD planning. Remember, it’s likely that employees are going to use their own devices at work whether you want them to or not. You might as well control it. In most cases, security should enable BYOD, not prevent it.

Accountability: Who is accountable for the device?

Users must understand the implications of a lost, misused or stolen device. IT should put in place the extra layers of security that enable BYOD, but ultimately users must ensure the success of the program.

Compliance: How will BYOD affect compliance?

If your industry is legislated or regulated, you must carefully consider how BYOD will affect the guidelines and SLAs. Keep in mind that BYOD has been successfully implemented in regulated corporations and the real concern is not the device, its lack of policy and procedure.

Application consistency: Can employees download at will?

Personal devices are designed for the consumer market and dictating what applications can or can’t download isn’t the best approach. Consider “containerization” a tool that creates and encrypted zone on a smartphone, or solutions offered by virtualized workspaces.

Unauthorized downloads: Can I avoid viruses?

BYOD devices should have the same download parameters as devices that are already on your network. You can also use edge security appliances and handle all BYOD devices as untrusted, forcing all to access corporate data and applications through the edge device.
Performance: How do I protect bandwidth?

Multi-media streaming, Internet radio and even gaming on BYOD devices can slow down network performance. In fact, the Allot Mobile Trends report\(^1\) showed that video streaming accounted for 42% of bandwidth usage. Strategies for protecting performance include setting policies for network use, creating separate networks and setting rules for giving priority to critical traffic.

Impact: What happens to our culture?

Will BYOD impact the company culture? Yes, but there’s little cause for concern. For example, Dell’s survey\(^2\) revealed that 54 percent of respondents believed BYOD positively impacted internal business culture and facilitated better teamwork.

Procedures: How do I communicate the plan?

BYOD procedures should be formalized and distributed with opportunities provided for users to ask questions pertinent to their device and their work/life situation. Procedures should outline policies for current devices, should be adaptable for future devices, and should enforce auditing and security policies.

Access: Is it foolproof?

No matter how good your BYOD deployment is, it won’t ever ensure that mobile employees will have access with their devices. Employees should have a backup plan for working and communicating while offsite.

Status Quo: Will it change our strategy?

Even if everything is moving along just fine in the infrastructure on a daily basis, BYOD means change. However, what most administrators already know is – it’s already happening, policy or not. As soon as an employee can access the corporate environment from their home PC or personal mobile device, that corporation has a BYOD situation. Therefore, the strategy has already changed.

---

BYOD the Worst Thing You Can Do Is Nothing

BYOD plans are never perfect - but key employees expect to be able to use their own devices for business. While BYOD presents some challenges to the organization, the worst thing a business can do is nothing. Asking the fundamental questions and addressing the fear, uncertainty and doubt that arise help IT staff map risks to potential solutions and workarounds. Ultimately, in order to get the most ROI from your BYOD program, you should consult a technology expert who can help you assess your unique needs and structure. After all, BYOD is happening with or without permission, it’s here to stay, and embracing a BYOD culture when possible can offer an organization a competitive advantage.

To learn more about how Glasshouse can help you optimize your BYOD strategy visit our website at www.glasshouse.com.

About GlassHouse

GlassHouse delivers vendor-independent consulting and managed services to guide customers through the complexities of cloud, workspace, security, and the data center (including virtualization and storage). GlassHouse does not sell any product, a principle that enables us to provide objective recommendations and integration strategies. We consider the people, processes, policies and technology already in place while creating a customized plan that mitigates security and non-compliance risks, improves cost and service efficiency, and enables IT departments to become true service providers for their organization. The depth and breadth of our expertise has been developed through more than 17,500 engagements with more than 12,000 clients. For more information visit www.glasshouse.com or visit the GlassHouse blog for expert commentary on key data center issues. Twitter users can follow us at @GlassHouse_Tech.