APPERIAN

An Apperian e-book

BRING YOUR OWN DEVICE: FROM SECURITY TO SUCCESS

INTRODUCTION

With 95% of organizations now permitting employee-owned devices in the workplace, the days of IT issuing corporate-owned devices are becoming very rare. The benefits of implementing a Bring Your Own Device (BYOD) policy have been established, meaning BYOD is no longer a trend. Rather, it is here to stay.

In order for your company to reap the rewards of BYOD a few important steps must be followed. For example, implementing new security measures for your corporate data and employee proofing your BYOD strategy.

This e-book was designed to walk you through best practices for executing a BYOD policy. It provides best approaches for data security, tips for employee-proofing your mobility solution, and an overview of what's next with BYOD 2.0. Plus, a bonus BYOD security webinar.

APPERIAN

TABLE OF CONTENTS

SECTION ONE: FOSTERING A BYOD ENVIRONMENT

BYOD has proven to provide benefits for organizations, from increased productivity to decreased IT costs. But to realize these benefits, BYOD programs must be implemented correctly. Below are some tips to follow to help ensure you are fostering a BYOD-friendly environment.

With mobile sales now officially outperforming PC sales -- and 95% of organizations permitting employee-owned devices in the workplace -- it's pretty clear to those of us in the industry that BYOD is no longer just a trend; it's established itself as a mainstay in the corporate environment. One of the reasons BYOD has taken off in recent years is that when implemented correctly, it benefits organizations as well as their employees.

BYOD is linked to increased productivity, higher levels of employee satisfaction, and decreased IT costs. According to a research study by Cisco Systems, BYOD solutions save enterprises up to $1300 per employee annually.

However, don't expect to reap the rewards of BYOD without first taking the time to create and foster a BYOD-friendly environment. This requires a holistic approach that extends beyond developing enterprise apps and enforcing mobile app security policies.

Get to know your workforce

You can't expect results from any BYOD initiative without first getting to know your workforce. Sit down with managers and employees from different departments to determine what they want to do on their devices. Chances are you'll uncover op-

portunities to maximize productivity that you never knew existed. Whether it's road warriors wanting to streamline expense reports or customer service agents asking for access corporate emails on-the-go, creating solutions and enterprise mobile apps in response to what employees want will go a long way in helping organizations to maximize the full potential of BYOD.

Don't force it

IT managers need to be careful not to force the issue with BYOD and avoid pushing for rapid mobile app adoption rates. In a multi-generational workplace, expect to see a wide range of different work habits. It comes as no surprise that Millennials are the quickest to adopt BYOD solutions and are especially drawn to social technology. Likewise, employees who aren't as comfortable wielding an arsenal of gadgets may be a little more hesitant to dive into enterprise apps head first. Organizations should respect these differences in work habits and understand that, in some cases, adoption takes time.

Maintain an open dialog

Mobile app security is the number one concern IT managers have about BYOD, but they're not the only ones losing sleep over the issue. Employees have their own worries about the implications of storing corporate data on their personal devices.

While it is vital for organizations to establish security policies to protect sensitive information, it is also important to maintain a level of transparency about such policies with employees. Establishing an open dialogue on the boundaries between personal and corporate data and what the organization expects from its BYOD-ers will help ease concerns on both sides of the fence.

Ensure scalability and sustainability with Mobile Application Management (MAM™)

Like any other IT project, to be sustainable BYOD solutions need to evolve over time to reflect the ever-changing business environment. In order to keep enterprise applications robust, plan for regular maintenance and updates. Centralizing administrative control over apps through mobile application management (MAM™) is the easiest way to keep them up to speed with the needs of the business. A MAM platform places app distribution, security, integration, and content management all within easy reach, allowing organizations to effectively manage their applications in support of a cohesive and productive BYOD environment.

SECTION TWO: CONTAINERIZED ENTERPRISE APPS & DATA

The shift from corporate-owned to personally-owned devices in the workplace calls for a change in how organizations secure corporate data. This section outlines a few of the most effective ways to keep corporate data secure without compromising employee privacy.

Back when smartphones mostly came in the form of company-issued Blackberrys, organizations benefited from a clear sense of ownership over their devices. Corporate smartphones were lent to employees for business purposes in the same way as desktop computers and laptops. This made creating mobile device management policies relatively simple. Then came the bring your own device (BYOD) movement and the need for BYOD solutions.

BYOD-Specific Concerns

BYOD has proven to be a sticky subject, as it can be difficult for organizations to navigate the fine line between corporate and personal ownership. The main issue with BYOD is that both personal and corporate data reside on the same device. When employees used company-issued devices, organizations could not only manage data, but also manage the device as a whole. This meant that if an employee lost a device or severed ties with the company, keeping data secure was as easy as remotely wiping all data off phone. However, this type of device management is simply not a viable BYOD solution.

Now that employees are using their own devices to perform work tasks, organizations must be mindful of their rights as device-owners when selecting BYOD solutions.

Threading the Needle with Containers

Among the available BYOD solutions, app containerization has risen to the top of the list as the best way to resolve the pesky issues surrounding ownership and jurisdiction. Through a series of technological features, containerized enterprise mobile apps allow corporate data to reside on personal devices while still under complete control of the enterprise. At the same time, BYOD owners remain fully in charge of their device and all of their personal data.

The most obvious benefit of having containerized apps is increased application and data security. Container technologies make it possible for IT security administrators to enforce a variety of security features specific only to enterprise apps. Such features can include single sign-on authentication, cut-and-paste restrictions, and app-level encryption. App containerization also allows for IT security managers to set broader security policies and push them out to applications. Together, all these features work to protect sensitive corporate data in case the device is lost, compromised, or the employee is no longer associated with the organization.

Best of Both Worlds

What app containerization offers is the best of both worlds: giving organizations the ability to manage and secure their enterprise apps at a granular level without infringing upon the rights of the device owner or sacrificing their user experience. It is a flexible and reliable BYOD solution that can be implemented in a variety of different ways, including via app wrapping or the SDK. Used in conjunction with mobile application management (MAM™), containerized apps allow both organizations and employees to enjoy the full benefits of the BYOD concept.

SECTION THREE: EMPLOYEE-PROOF YOUR MOBILITY SOLUTION

Allowing employees to access corporate data on personal devices inherently can be risky, but BYOD can be rolled out with extremely high levels of security. Below are suggestions on how to employee-proof your enterprise mobility solution to ensure you won't jeopardize corporate information.

When you have a BYOD (Bring Your Own Device) policy at your company, you are allowing your employees to use their devices at work, where their personal apps, settings, and usage can end up jeopardizing your client information and introduce the possibility of a data breach. But you don't have to abandon BYOD to keep your company safe -- there are ways to employee-proof your enterprise mobility solution.

Create Your Own Apps

One way to employee-proof your enterprise mobility solution is to develop your own enterprise apps. This will help your employees achieve efficiency because they are using applications best suited to your business. It also ensures compatibility with your company's hardware, software, and data storage while removing the risks to your business that is often inherent with 3rd party apps.

In order to have an effective mobile application management (MAM™) policy, your organization has to determine which enterprise apps they want to create and ensure that your employees use them over 3rd party apps.

Start with which apps your employees seem to use the most for work and how they could be altered to suit your company needs. This can even mean merging the ideas

of several apps together can help create an efficient way to help your employees communicate, work, and effectively help your customers.

Have employees and management create a list of what type of apps they want to see and what they want these apps to do. This helps your IT team create an effective to-do list as they look at app development and management. Lastly, asking for input will also make employees willing to use the applications once they are created.

Use Employee-Friendly Controls

Another benefit to an app-centric enterprise mobility solution is that it helps to resolve the conflict many organizations have with their employees and personal information.

When you try to handle BYOD policies at the device level, employees will feel that you are infringing on their privacy. This may mean that they will seek workarounds to any security measures you try to employ and this can create a risk to your company's important data.

By implementing a mobile application management solution, your company can protect proprietary information with secure enterprise mobile apps and can leave the rest of the device alone. The employees won't feel like Big Brother is parked on their cell phones and your company can be secure in the knowledge it has protected business applications.

Communicate

The difference between BYOD strategies and device management strategies is that you have to acknowledge that employees have both personal and business information on their mobile devices. There will be concerns about what information your company is accessing, restricting, and removing with its management policy.

In order to foster mobile app adoption with your enterprise mobility solution, your company should create terms that are detailed, transparent, and fluid. Always explain what you are doing to your employees and why -- and as times change, your employees' usage patterns will change as well. When you communicate with employees about how they use their mobile devices for work, you will be able to adopt your BYOD policies to keep your stakeholders happy, your data safe, and make your employees more efficient.

SECTION FOUR: BRACING FOR BYOD 2.0

Your BYOD policy is in place and your employee's needs are satisfied, but what is next? BYOD 2.0 is aimed to align the needs of your employees with the needs of the enterprise. Learn how to achieve a win-win mobile environment that drives employee productivity and satisfaction below.

A growing number of industry experts maintain that we're in the era of bring your own device (BYOD) 2.0 where the needs of the employee and the enterprise are coming into full alignment. In a clear distinction made by Bob Egan in a post for Forbes, "If BYOD 1.0 has been responding to the needs of the employee, BYOD 2.0 efforts will focus more on where the the needs of the enterprise and the employee intersect. Perhaps the most valuable key attribute of BYOD 2.0 will be to provide right-time experience (user interface + user experience) to the systems, solutions and points of collaboration that are mutually relevant to the company and to the employee."

We couldn't agree more. In fact, we would take this a step further by underscoring how BYOD works most effectively when there is clear mutual benefit to both the employee and to the company. When companies are able to provide employees with an enterprise app store that's easy to navigate, find, and download applications, both the company and employees win.

As companies develop more enterprise mobile apps, their IT organizations will

also need to strike a balance between putting in place mobile app security policies that protect the organization and its customers from misuse of proprietary data via malware, trojans, viruses, etc. without crafting policies that are too wieldy or draconian for employees to abide by. This will become even more important as employees expand their use of enterprise apps beyond mobile email and adopt other types of productivity-enhancing apps such as mobile CRM, mobile ERP, mobile sales automation, or field service tools, etc.

An enterprise mobility solution focused on mobile application management (MAM™) can address the convergence between satisfying the needs of both employees and enterprises. Our MAM platform is designed with the kind of flexibility that makes it easy for employees to locate and use the types of mobile tools that can help them do their jobs better while providing IT with a level of automation and sophistication that makes mobile management easy and logical. Using MAM, companies can provide employees access only to those apps that they are qualified to download based on their roles. Meanwhile, as the BYOD 2.0 era ushers in countless new productivity-enhancing apps for companies to exploit, employees can rest assured that their personal data won't be disrupted on their devices.

APPERIAN

WEBINAR: MOBILE SECURITY WITH BYOD EMPLOYEES LOVE

When done right, BYOD can increase employee productivity and workforce satisfaction, while maintaining the security you need. Watch this webinar to learn how to drive mobile security and support the BYOD your employees love.

Gartner predicts that by 2017 more than 50% of companies will have implemented a BYOD (bring your own device) program. Whether you already have BYOD, or are planning for your BYOD future, security is likely one of your top concerns. Fortunately, when done right BYOD can increase employee productivity and workforce satisfaction while maintaining the security you need.

Unfortunately, many companies often struggle by implementing BYOD policies that are too intrusive to end-user's personal devices. The business results and security benefits are lost altogether.

In this webinar Carlos Montero-Luque, Chief Technology Officer at Apperian reveals:

- Why focusing on the true end-point of mobility, the apps and data, is the best approach to create a secure BYOD environment
- How a zero-touch, non-intrusive BYOD security approach increases employee productivity
- What practical steps you can take to simplify the complexity of supporting multiple devices, operating systems, and contingent workforce BYOD environments.

WATCH THE WEBINAR

To stay up-to-date with mobile research and trends follow us on LinkedIn