BEACHHEAD

Whitepaper

3 Common Mobile Security Mistakes

Failure to consider basic objectives will require resources, impede employee productivity ***and*** cost you money

Gerald Hopkins
Cam Roberson

May 2013

Introduction

Simplified objectives often forgotten in rush to plug mobile data leakage

This whitepaper investigates the dynamics of the mobile device market particularly in light of the rapidly developing BYOD ("Bring Your Own Device") phenomenon. Most importantly, we look at the mistakes often made by businesses (especially small- and medium-sized business) when decisions on how to address security of these devices are made hastily, even desperately as they attempt to address this fundamental workplace transformation. Failure to properly weigh these mobile device considerations can lead to a purchase that is costly, demands infrastructure support and maintenance and that encumbers employee productivity. In many cases the hit to productivity can be so extreme so as counteract entirely the very benefit that BYOD brings to business. More often than not, businesses falsely believe that they must employ hardware and tools that are engineered for large enterprise and in many cases are just too complex and burdensome for organizations with already stretched IT staff and budgets. This whitepaper views this issue through the spectrum of the two most important objectives of business in addressing the BYOD phenomenon. First, businesses would like to enable the productivity gained when employees choose and bring their own mobile device. Secondly, the organization realizes that it is essential that while employees access business data that business have control over that data ensuring that it remains secure and confidential.

Rapid Change = Burgeoning Risk

Data security risks have proliferated under watchful eye of regulators & lawmakers

Not very long ago, IT professionals wielded nearly absolute authority over all their companies' devices: Maintaining oversight of PCs and laptops and even some mobile devices with data capabilities (like Blackberry smartphones) was a relatively easy task. In the great majority of cases, companies owned the hardware used by their employees and they exercised control over the data contained on them. It was a pretty black and white matter, but with the emergence of mobile devices with greater data capabilities, what had been a black and white matter has become increasingly gray as more and more employees are bringing their own devices, with robust data capabilities, into their workplaces. As this trend picks up momentum, IT professionals are seeking to implement solutions that allow them to maintain control over corporate data. And for good reason: With the increased capabilities of these BYOD devices comes increased risk, and properly addressing such risk is of the utmost importance. Unauthorized devices accessing, storing, and disseminating sensitive data poses obvious risks, with increasingly grave consequences. For example, newly implemented data protection provisions of the Health Insurance Portability and Accountability Act (HIPAA) could impose penalties of $1.5 million per violation. No longer are small and medium businesses immune to these penalties. This year, the Department of Health and Human Services (HHS) imposed a $50,000 fine on The Hospice of North Idaho for a breach involving less than 500 records of confidential patient health information resulting from a compromised mobile device.

It's clear that enterprises are appreciative of these risks, evidenced by rapidly increased adoption of mobile device management ("MDM") solutions. Selecting the right solution is critical.* This paper discusses three common mistakes IT managers commonly make when assessing risk, and deciding how to address it.

*A recent survey by Gartner revealed that two thirds of enterprises will have adopted MDM solutions by 2017.
http://www.gartner.com/newsroom/id/2213115

Mistake #1: Over-thinking (Don't Over-Think It!)

Allow BYOD *and* protect business data

In assessing all possible risks to sensitive corporate data, it's easy to understand why IT professionals might feel overwhelmed. In the past, IT policies had typically been a "top-down" proposition, with management making decisions about hardware and software procurement, including decisions about security and device management solutions. The BYOD/consumerization trend has turned that notion on its head, and companies are scrambling to address the consequences of individual hardware and software decisions made by their employees. The threats to corporate data seem to evolve more quickly each year, and IT professionals who aren't well versed in mobile operating systems might believe that special expertise is required to address the threats posed by smartphones, tablets, and other mobile devices. In reality, addressing security requirements of mobile devices shouldn't be complicated at all. After all, smartphones and tablets should really be considered just different varieties of computers, even if smaller. There is often a tendency to take an overkill approach to managing mobile devices, implementing restrictive, over-engineered solutions that hinder both the rich user experience typically afforded by the new generation of mobile devices (iOS and Android devices in particular) and, even worse, restrict productivity. BYOD is a trend that is here to stay, and enterprises should embrace the trend and its benefits of ubiquitous employee connectivity and productivity as long as corporate data is secured. And there's no reason that enterprises can't have it both ways: Productivity and security should never be mutually exclusive. Ultimately, enterprises should look to implement solutions that protect their data assets and ensure legal/regulatory compliance while taking advantages of the many benefits of the BYOD trend.

Mistake #2: Too Many Different Device Management Solutions

Despite the trend toward BYOD, traditional computing devices remain integral productivity devices in enterprise environments - Macs and PCs are here to stay! Consequently, IT professionals are going to have to contend with management requirements for both traditional devices (PCs, Macs, laptops) and mobile devices for the foreseeable future. As mentioned above, there is often an erroneous tendency to think of mobile computing devices as being very different from traditional computing devices like PCs and Macs. Again, in reality, they are just small computing devices with different operating systems. Nevertheless, some IT professionals might believe that different operating systems or different platforms require different solutions to manage them. Implementing different management solutions is certainly possible, but it is also extremely inefficient and not necessary. The training required to install, operate and maintain different device management solutions imposes a burden on IT personnel in terms of time. And in assessing available hardware management solutions, IT professionals should strongly consider unified management solutions, capable of managing as wide an array of device types as possible.

Mistake #3: Effective Solutions Must be Expensive

Most are built for large enterprises with big budgets

No one wants to overspend for anything – especially if you're an IT professional making purchasing decisions for your company. But overspending is easy to do if one isn't apprised of all the facts and hidden costs associated with purchases. In the context of BYOD device management, IT professionals might be tempted to purchase security appliances (rather than licensed solution or paying for subscriptions services) believing that a one time investment is the most economical approach. But buying (as opposed to using subscription services) also comes with its own risks: A purchased solution likely carries annual maintenance fees in the form of a sizable percentages of the purchase price. And as technology evolves, and requirements change, a buyer might soon find that what had seemed to be cutting-edge technology is now obsolete, and they are then saddled with a white elephant that can't address new requirements. It's also possible that a vendor may charge additional fees for new management modules or capabilities. *Caveat emptor* (Buyer Beware) is pertinent advice in the device management market. Subscription services for device management can very often be a better approach, providing enterprises the comfort of knowing that there are no hidden costs, and that the services they are paying for will evolve with technology innovations and requirements.

SimplySecure™ Mobile Device Security

Self-managed or a monthly managed service

Beachhead's SimplySecure™ Management System is an entirely cloud-based ecosystem that provides security and control over your inventory employee- and company-owned iPhones, iPads and Android phones and tabs. SimplySecure is a cost-effective solution that squarely addresses the key objectives of a business facing the challenges of a mobile workforce accessing and manipulating company sensitive data. Specifically, SimplySecure allows you to embrace the productivity benefits of a BYOD workforce while ensure the security of your sensitive data. Your data is "Simply Secure." Employees are not encumbered with different processes or authentication nor do they need to learn special software or use specific applications. While most MDM offerings are built for enterprises who can draw upon ample resources, SimplySecure neatly meets the objectives of small and medium sized business.

But aren't PCs and Macs mobile too? And what about USB storage? Shouldn't business be concerned about these ubiquitous and high-capacity data repositories? The SimplySecure Management System is a unified console enforce encryption and manage security on "All Things Mobile.

This protection service can either be self-managed or managed on your behalf by highly trained IT service professionals that have earned "Beachhead-authorized MSP" recognition. Qualified IT professionals using this powerful cloud-based tool secure your mobile devices as an affordable monthly service with no impact to your business or employee productivity.

BEACHHEAD

Beachhead Solutions Inc.
1955 The Alameda
San Jose, CA 95126

408.496.6936

Question, comments? Write Cam Roberson

croberson@beachheadsolutions.com