keeper

How to

Provision Employees in a BYOD World

White Paper **2016**

Introduction

A December 2014 study from Gartner, Inc., found that more than 50% of consumers will use a tablet or smartphone for all online activities by 2018[i]. The stunning rise and adoption of mobile technology far exceeds anything that came before it. In 2011, for example, 35% of Americans owned a smartphone; today, nearly 70% own one. As researchers at MIT noted, "the only technology that moved as quickly to the U.S. mainstream was television between 1950 and 1953.[ii]" And now consumers watch television on their smartphones and tablets.

Given the pace of the IT consumerization it makes sense that employers would want to accommodate workers' desire for convenience and mobility. The number of organizations that allow their employees to use personal devices for work-related reasons (otherwise known as BYOD) is one of the fastest trends in business today. Employers clearly appreciate the cost-savings associated with BYOD policies, while employees appreciate not being chained to a desk. In fact, so popular have BYOD policies become that Gartner found that by 2016, 38% of companies expect to stop providing devices to workers[iii]. By 2017, half of companies will require employees to bring their own device. In other words, when it comes to BYOD, we're moving from convenience to something that will be mandatory.

Consumers are often employees. Personal mobile devices are being used for business email, social content and commerce. Companies face a serious challenge of figuring out how to manage and secure these devices noting they don't own them. This is the big problem.

An unfettered, unrestricted BYOD policy exposes an organization to massive security risks. In an age when even the most security-savvy organizations can be the victims of hackers and information thieves, no organization should adopt a BYOD policy without a thorough risk assessment and security strategy. This white paper will inform organization heads about the risks associated with any BYOD policy and suggest appropriate steps to ensure that an employee's smartphone won't become the key that unlocks an organization's data kingdom.

Key Insights

In this white paper, readers will:

- >> Learn about the cyber-security risks associated with BYOD.
- >> Discover why employee provisioning presents the first line of a sound, proactive defense in an organization's BYOD strategy.
- >> Understand the core elements of protecting an organization's sensitive data.

Bring Your Own Device Brings Its Own Risks

In many ways, BYOD represents the future of workplace employment. The era of office- or cubicle-bound employees is quickly transitioning to a more mobile, more connected cyber-workforce. Driving this change is a fundamental element of today's technology: choice, or the ability to work in a way that leads to greater productivity and more convenience. Choice, when matched with near-ubiquitous 4G networks and ever-present WiFi, means that "work" broadly defined is no longer determined by location; rather, it's determined by activity. One can work anywhere on a variety of devices that best meet his or her needs. Employers certainly appreciate how BYOD helps build a happier, more productive workforce. But they probably enjoy the cost-savings a bit more. When implemented correctly, a basic BYOD policy on average saves a company about $350 per employee per year, according to a Cisco analysis. A more comprehensive BYOD policy can yield upwards of $1,650 in annual savings per employee[iv].

But the new digital economy, of which BYOD is a result, has a very dark underside. The rise of greater choice and mobility in the workforce correlates strongly with the rise of cyber-crime, whose sheer scale is mind-boggling. The British insurance company Lloyd's estimates that cybercrime costs businesses $400 billion every year[v]. Indeed, at the World Economic Forum in Davos in January 2015, where cyber-security was the preeminent issue, Accenture CEO Pierre Nanterme said the "four biggest challenges the tech industry faces in coming years are security, security, security and security."[vi] In a ZDNet.com survey of 400 IT professionals, 96% said that security was extremely or somewhat important to IT departments over the next three years, by far the top response. Just beneath it at 89%, was mobile device management, which is an issue created by BYOD.

Which is why it's surprising how ill-prepared most companies are when it comes to cyber-security and BYOD policies. According to EY, fewer than 20% of organizations have real-time insight on cyber-security risks readily available[vii]. Meanwhile, a 2014 survey last year by TEKsystems of 2,000 IT professionals found that 38% thought more than half their companies' sensitive data was at risk and 20% thought all corporate data could be compromised because of BYOD[PG1] .

Part of the problem is that many organizations' BYOD developed organically. What first might have started as employees simply checking their work email at home or on their smartphones turned into permission to access a company's otherwise secure enterprise system remotely (even if it's inside the office). Organizations whose BYOD practices have evolved over time probably haven't properly assessed the risks and likely don't understand how exposed their systems really are. The larger the organization, the bigger the problem an evolving BYOD policy is.

Yet the rise of IT consumerization now means that even the smallest of companies can adopt a BYOD policy – and in many ways, it makes perfect sense to do so. Big, small, or medium, the cyber-security risks that come with BYOD are roughly the same in type if not in scale and boil down to a simple rule: every organization that permits its employees to use their own devices for work-related purposes must understand the security risks and protect their systems accordingly.

What Are Those Risks?

Stolen Device

The most obvious risk with BYOD is what happens when an employee's device is stolen. When three-out-ten smartphone owners don't use passwords to access their device[viii], the problem for businesses becomes acute. An unprotected smartphone with access to a company's systems is a disaster waiting to happen. It doesn't help that even those consumers who use smartphone or tablet passwords probably choose easily hackable passwords. According to Entrepreneur magazine, 90% of employee passwords can be hacked in six hours. Moreover, 65% of U.S. adults use the same password for all of their accounts[ix]. In a BYOD world a single stolen smartphone is a major inconvenience for the consumer; it can be catastrophic for a company.

App Downloads

The very idea of a mobile malware attack is still inconceivable to most consumers, who on average don't apply the same protections to their smartphones and tablets as they do to their desktops and laptops. But it's only a matter of time before a major attack occurs. For example, in February 2015, Google removed three apps from the Google Play store because they presented security risks[x]. As a report from Lookout found, mobile malware encounter rates shot up by 75% in 2014 within the U.S.[xi] In an enclosed IT world, where every employee has a company-issued desktop or laptop, restricting downloads and web-site access is relatively simple; in a BYOD world, it becomes a logistics nightmare.

WiFi Insecurities

Companies considering a BYOD policy might make the mistake of thinking that because they have security measures in place governing the use of laptops off-site, then they're protected with other mobile devices. But laptops work much differently than mobile devices. For starters, smartphones and tablets are almost always "on" – connected or searching for WiFi and constantly using 3G or 4G networks. Smartphones in particular are incredibly insecure and easy to hack. For example, at the 2015 Mobile World Congress in Barcelona, Avast Software set up a faux-fraudulent wire less hotspot at its booth that immediately "infected" any mobile device that came in its vicinity with tracking software[x ii]. Consumers rarely think about the network to which their devices are connecting, and often they won't even know if their smartphone has been hacked. But an infected smartphone or tablet that then connects to an organization's system is like a cyber-age Trojan Horse.

Employee Carelessness

There are multiple risks that fall into this category. Put simply, when an organization no longer "owns" the device with which the employees works, then it's very hard to make that employee practice good device behavior. This includes, but isn't limited to, downloading software security updates; restricting app access to user data; and ensuring that company data doesn't get uploaded on cloud-based storage systems, like DropBox or Google Drive. Employee carelessness on any of these can expose sensitive organizational data and/or open a door for a hacker to get inside the system.

What Are Those Risks?

Employee Maliciousness

Yes, there are selfish, disgruntled, and otherwise bad employees who would use a company's lackadaisical BYOD policy to do harm. For example, tech-savvy employees can "jailbreak" (iPhones) or "root" (Android) their devices. The two terms are essentially the same and mean that a user has bypassed the device's built-in administrative restrictions. This gives the user the ability to download apps and software that an otherwise normal smartphone or tablet would reject, then doing all sorts of mischief when connected to the organization's systems. And the mischief isn't isolated to the employee's tenure at the organization. According to an Intermedia survey, 89% of respondents retained access to at least one application from a former employer[xiii].

The good news? These risks are all preventable or at least manageable if an organization places cyber-security at the center of its BYOD policy. And because the employee – or rather, the employee's device – forms the very heart of BYOD, then it makes sense that any active defense against the cyber-crooks begins with the employee.

Employee Provisioning: The First Line of Proactive Defense

To put it bluntly, employees will never take an organization's cyber-security as seriously as they should. They will do what they need to do to stay within the BYOD rules and regulations of the organization but no more should be expected. A recent study from Aruba Networks[xiv], which questioned over 11,500 workers across 23 countries worldwide, bears this out. Some eye-popping findings from the study include:

- Employees placed "security" fifth behind brand and operating system when making buying decisions for new devices.
- 87% assume their IT departments will keep them protected, yet nearly a third (31%) have lost data due to the misuse of a mobile device.
- 39% of respondents from financial institutions admit to losing company data through the misuse of a mobile device, which is 25% higher than the average across all industries surveyed.
- 56% of workers today said they are willing to disobey their boss to get something done, while six in ten share their work and personal devices with others regularly.
- Lastly, nearly a fifth of employees don't have passwords on devices, with 22% of those stating they don't have security measures in place so that they can share more easily.

Certainly variations in employee attitudes to cyber-security exist depending on the size of the organization. Employees at smaller organizations have more to lose in the event of a catastrophic data breach, while those at larger organizations likely believe that a breach won't affect them. Regardless of size, however, an organization must assume that employees won't make security a top priority.

This is why the provisioning phase of an employee's onboarding becomes takes center stage in an effective, secure BYOD policy. During the provisioning phase, employees usually receive their email accounts and database and application access – in other words, everything that a cyber-crook would love to get his hands on. It's during this phase also that an employee chooses a password to manage access and is told of the policies and regulations that apply to accessing company information.

Provisioning is also when an employee receives whatever equipment he or she will need: desktop or laptop, phone, etc. Assuming the organization makes security a top-priority, these machines will already have security measures in place. These rules and regulations might be automatic (e.g, restricted sites or downloads) or require the employee to exercise good judgment.

But in a BYOD world, the provisioning process changes. For starters the company will need to check and register the employee's devices he or she would use for work. Also, whatever software the organization uses will have to be installed on the device, including security software. Finally, the employee will have to be guided through appropriate and unsafe device behavior – as well as the consequences for engaging in unsafe behavior.

The simple reality is that BYOD puts a heavy share of the security responsibility on the employee. This is why the provisioning phase marks the first line of defense in any organization's BYOD policy. In some ways, BYOD is an agreement between employee and employer, because both are required to do their part to reap the benefits of BYOD and minimize the risk. But as we've seen, employees normally don't take security as seriously as they should. Worse, there's no way for an employer to know a particular worker's dedication to company security until it's too late. In an era when the hackers are always one step ahead of the defenders, an organization is always gambling at some level.

This is the critical question: How can an organization minimize the risks from BYOD without relying on an often indifferent workforce?

A Three-Pronged Solution to BYOD Security

The best strategy for a safe and effective BYOD policy is to remove as much of the security decision-making from employees as possible. We hasten to add that this shouldn't be seen as a negative decision (i.e. you won't be restricting your employees' freedom to use their personal devices), but rather a decision that allows a business -- executives, managers, and employees -- to get the most out of a BYOD model that seeks to maximize employee performance, happiness and organization security. What follows are three effective tactics that any organization either with an existing BYOD policy or looking to implement one should follow to the benefit of all:

Password Management

Put simply, a laissez-faire attitude to employee-chosen passwords is a security hazard. Even if an organization requires a specific number of letters, numerals, and/or symbols, it still runs the risk that an employee will choose a password he/she uses on personal accounts. The solution is to take the choice out of the employee's hands with a password management system, which securely stores through encryption all of a user's passwords. PM systems also allow a user or organization to sync across all devices. Some features to look for in an enterprise-level PM system include:

Password management systems allow employees to randomly generate passwords, which can be calibrated to fit an organization's desired level of complexity. An organization therefore can require multiple passwords, all randomly selected, for multiple systems. The user accesses these systems via the password management system and after he or she has entered a master password, which he or she can choose or be assigned. Employees must choose a strong password that meets enforced password guidelines, but otherwise they won't have to remember another password for any company needs, reducing the password-reset requests that often plague IT departments. Furthermore, most password managers provide auto-fill, so that an employee doesn't need to remember the randomly selected password.

The auto-fill feature, while convenient, also represents a security risk without a self-destruct feature after a certain number of failed attemps to login. Two-factor authentication eliminates this risk by requiring the authorized user to have something to gain complete the authentication process. Sophisticated password management applications offer multiple two-factor authentication methods including RSA SecureID which is used as a token at thousands of enterprises. Enterprise-level password managers should also come with an admin console that allows new users to be added and removed quickly and efficiently and enforce security settings for individual employees.

The ability to enforce policy controls, define access roles and restrict sharing is critical for safe enterprise password management. Limiting employee access ensures that employees only have company resources and logins that they need at the times that they need it, greatly reducing the risk from careless or disgruntled employees. Assigning a delegated admin that is regularly monitoring, provisioning and deprovisioning access to users based on their role in the company is highly recommended.

VPN (Virtual Private Network)

Sending and receiving data across insecure networks is one of the biggest concerns with BYOD. Consumers often have little regard for the type of network through which they're sending or receiving data: a coffee shop, an airport, public WiFi, etc. A competent hacker can easily steal this data, as well as hack into an organization's system, via an insecure network. A VPN provides a secure, encrypted tunnel that allows safe data transmission between an off-site employee and a company that third parties cannot intercept. Many VPNs, although not all, also offer a "dynamic firewall" that allows the employee to use nearly all types of network environments, particularly vulnerable access points like public WiFi. During the provisioning phase, an employee's mobile device(s) would be equipped with access to the organization's VPN. An additional security measure would be to have "per-app VPN," which helps organizations lessen the risk of employees downloading malicious apps. This type of VPN allows only approved apps to access the organization's network and resources.

The ability to enforce policy controls, define access roles and restrict sharing is critical for safe enterprise password management. Limiting employee access ensures that employees only have company resources and logins that they need at the times that they need it, greatly reducing the risk from careless or disgruntled employees. Assigning a delegated admin that is regularly monitoring, provisioning and deprovisioning access to users based on their role in the company is highly recommended.

EMM (Enterprise Mobility Management))

In BYOD's earlier days, organizations used mobile device management (MDM) software to monitor, manage and secure employees' mobile devices. MDM allows an IT department to manage an employee's mobile device by first registering the device and installing the appropriate software during the provisioning phase. A second feature of MDM is that an IT department can access the device remotely to troubleshoot problems or even, in the event of a lost or stolen device, wipe the device.

The software has evolved to include content and app management to form the more comprehensive EMM. App management generally involves installing an employee's basic systems: email, calendar, and contact information. It also includes installing app extensions that govern what apps the employee is allowed to download to his or her

device. Content management governs how an employee can store, access, and send and receive data. This allows the organization to restrict how the employee is using the content that he or she accesses and ensure that all content is kept secure, even when the employee is not on the organization's network.

Constant Vigilance

BYOD security is not limited to these three solutions, but they remain critical steps in any organization's BYOD policy that it can implement during the provisioning phase. In other words, before an employee receives his or her first company email, an organization can be confident that the employee's mobile device is safe for use. Keep in mind that registering, managing, and tracking the dozens, hundreds or even thousands of devices that come with a BYOD policy can frustrate even the savviest of IT departments. These three solutions help streamline the process, secure organization data, and remove most employee carelessness or maliciousness from the equation. And yet an organization can still reap the cost-savings and convenience that come with a BYOD policy.

However, when it comes to cyber-security the world is becoming more dangerous, not less. Even as new technologies and software help organizations realize tremendous results, those same tools are being used to undermine the global economy. What's worse is that far too many organizations make it easy for hackers to steal their critical information. Together, we must fight back against the cyber-criminals and make the latest technology work for us, not against us.

This is why no solution, however reliable today, lasts very long. Organizations must remember that the best way to keep itself and its employees safe is through constant vigilance of the technology available. Remember: what technology solutions are commercially available to organizations today were available to the hackers yesterday.

About Keeper Security

Keeper Security is transforming the way businesses and individuals protect their passwords and sensitive digital assets to significantly reduce cyber theft. As the leading password manager and digital vault, Keeper helps millions of people and thousands of businesses substantially mitigate the risk of a data breach. Keeper is SOC 2 Certified and utilizes best-in-class encryption to safeguard its customers. Keeper protects industry-leading companies including Sony, Chipotle, and The University of Alabama at Birmingham. Keeper partners with global OEMs and mobile operators to preload Keeper on smartphones and tablets.

Contact

850 W. Jackson Blvd. Suite 500
Chicago, IL 60607

keepersecurity.com

312.829.2680

sales@keepersecurity.com

Resources Cited

[i] http://www.gartner.com/newsroom/id/2939217

[ii] http://www.technologyreview.com/news/427787/are-smart-phones-spreading-faster-than-any-technology-in-human-history/

[iii] http://www.gartner.com/newsroom/id/2466615

[iv] http://blogs.cisco.com/news/new-analysis-comprehensive-byod-implementation-increases-productivity-decreases-costs

[v] http://fortune.com/2015/01/23/cyber-attack-insurance-lloyds/

[vi] http://fortune.com/2015/01/22/cybersecurity-fears-put-a-chill-on-the-davos-feelgood-vibe/

[vii] http://www.ey.com/GL/en/Services/Advisory/EY-global-information-security-survey-2014-activate

[viii] http://www.cnn.com/2013/02/26/tech/mobile/smartphones-passwords-mcafee/

[ix] http://www.entrepreneur.com/article/242208

[x] http://www.digitaltrends.com/mobile/google-removes-adware-app-from-google-play/

[xi] https://www.lookout.com/static/ee_images/Consumer_Threat_Report_Final_ENGLISH_1.14.pdf

[xii] http://www.bloomberg.com/news/articles/2015-03-02/the-easiest-way-to-get-hacked-use-phone-at-phone-show

[xiii] http://www.intermedia.net/Reports/RogueAccess

[xiv] http://news.arubanetworks.com/press-release/enterprise-security-threat-level-directly-linked-user-demographics-industry-and-geogra?_ga=1.217886358.1440923962.1430513102