blancco

WHITE PAPER

Mobile Data Erasure: Preventing Enterprise Data From Going Rogue

A Brave New & Insecure Mobile World

It has long been said that an organization's greatest asset walks out the door every evening—a reference to the tremendous value of human capital. But there's another invaluable asset exiting the building along with your employees: your mission-critical corporate data.

Mobile devices, once a luxury and now a daily necessity, are transforming the way employees access, use and share enterprise data. Gone are the days when employee records, customer information and intellectual property remained locked inside the data center. In the olden days when mobile devices were still in their infancy, that data store was then extended to departmental servers and desktop computers. Today that information trove is now stashed in workers' pockets and purses, accessed and stored on smartphones and tablets.

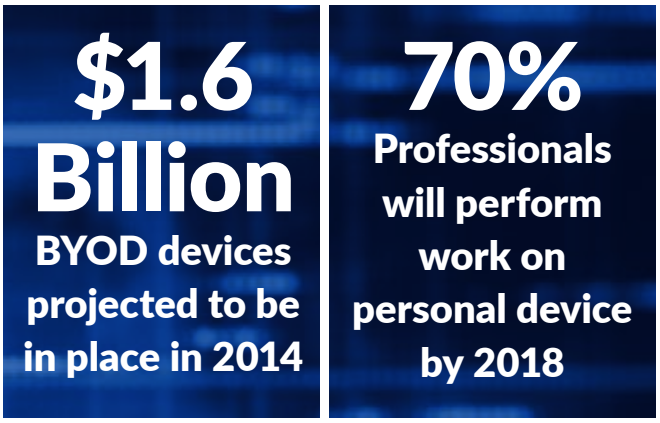
This brave new mobile world has inevitably raised the bar on data security for a number of reasons. First, information on mobile devices is harder to track and manage. Second, these handheld devices make it that much easier to be hacked, lost or stolen. What's more, the risks persist not only while the devices are actively used in your enterprise, but also when they're discarded or resold in the secondary market.

Many users—as well as enterprise businesses—mistakenly assume that manually deleting data or performing a factory reset will wipe a mobile device clean and eliminate any potential security threats. But that is just not the case. These actions simply remove pointers to where the data resides. The hard truth is that this type of "deleted" data can quickly and easily be recovered—and when it falls into the wrong hands, could have very dangerous consequences for enterprise businesses, their employees and their customers.

The solution more and more organizations are waking up to is mobile data erasure – achieved through enterprise-class software that truly erases, and verifies the erasure of, your mobile data. Here's how to leverage mobile data erasure to help protect your organization's information assets.

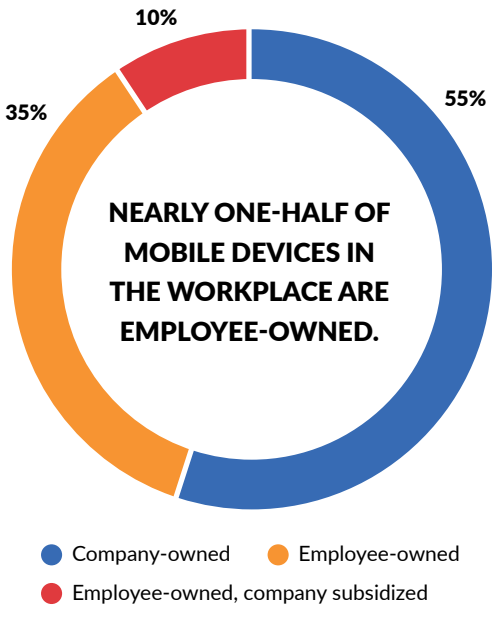
Bring Your Own Data Leak

It's no secret that the use of mobile devices in the workplace has exploded. And a growing proportion of that equipment falls into the BYOD category. According to Gartner, it's estimated that there would be 1.6 billion BYOD devices in use by 2014. And nearly half of mobile devices in the workplace are now employee-owned, reports Spiceworks. (See Figure 1.) Now consider this: By 2018, fully 70 percent of professionals will perform work on a personal device, says Gartner.



Source: "Bring Your Own Device: The Facts and the Future," Gartner, May 2013

Figure 1: Mobile Device Ownership in the Workplace

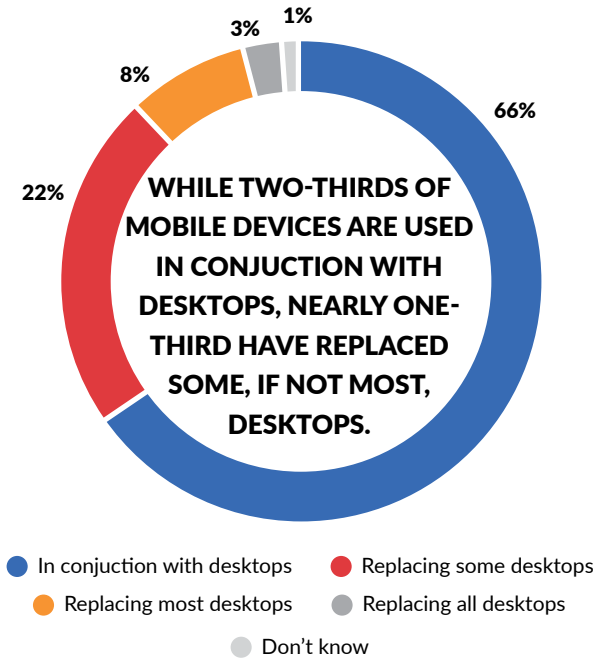


Source: "The Rise of the Mobile Empire," Spiceworks, April 2015

1 "Bring Your Own Device: The Facts and the Future," Gartner, May 2013
2 "The Rise of the Mobile Empire," Spiceworks, April 2015
3 "Bring Your Own Device: The Facts and the Future," Gartner, May 2013

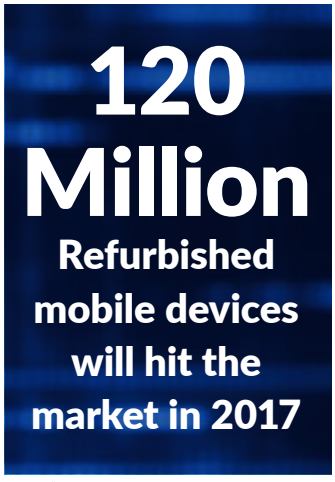
These devices are now a key means of accessing and storing corporate data. While two-thirds of mobile devices are used in conjunction with a desktop, nearly one-third of mobile devices have replaced some, if not most, desktops. (See Figure 2.) In fact, use of desktop computers will increase only 15 percent in the next three years, but use of tablets will leap 75 percent. (See Figure 3.)

Figure 2: How Mobile Devices Are Used



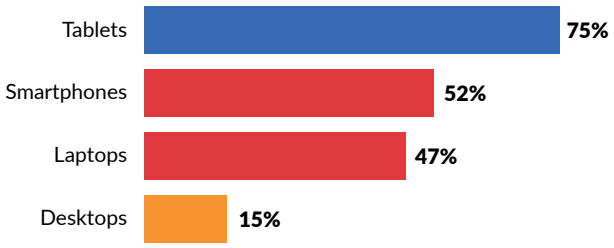
Source: "The Rise of the Mobile Empire," Spiceworks, April 2015

But it's not only the devices currently in your enterprise that should be of concern. You also need to think about what will happen to corporate data after mobile devices are retired and remarketed for use in secondary markets. Due to increasing demand for product development and innovation, the replacement cycle for smartphones and tablets is getting shorter and shorter, which is driving continued sales growth in the second-hand mobile device market. In fact, Gartner estimates the market for refurbished



Source: "Reused, Resold, Recycled: Where Do Smartphones Go?," Gartner, February 2015

Figure 3: Increase in Device Use in Next Three Years



Source: "The Rise of the Mobile Empire," Spiceworks, April 2015

mobile phones will nearly double from 56 million units in 2014 to 120 million units in 2017.

Data Erasure, Anywhere & Everywhere

Amidst all of these factors, there is still a light at the end of the tunnel. The good news is that more organizations recognize the need for mobile data erasure. To better understand the opportunity that exists, we will outline several trends contributing to this rapid growth in mobile adoption and popularity.

Exploding Data: Organizations manage an ever-expanding amount of data stores. How big, you might ask? According to the International Data Corporation, the global volume of data will mushroom from 4.4 zettabytes (ZB) in 2013 to a staggering 44 ZB—that is, 44 trillion gigabytes—in 2020. In other words, it's massive. More and more of that data—from employee records to customer information to intellectual property—is ending up on mobile devices. After all, mobile devices are essentially computers with a small screen; the average smartphone has more processing power than the equipment that landed Apollo 11 on the moon. And what's more interesting is that many tablets can now store 128 GB of data, which can include anything and everything from customer names to sensitive financial information to confidential emails to passwords and so much more.

Escalating Cyber Attacks: As users shift from their bigger laptops and desktop computers to their more lightweight, sophisticated smartphones and tablets, the targets of cyber attackers are shifting along with them. In the first half of 2014 alone, 175,442 new, unique pieces of Android malware were detected, according to Kaspersky Lab—that's an 18 percent leap over the entire year of 2013. Between August

4 "Reused, Resold, Recycled Where Do Old Smartphones Go?", Gartner, February 2015
5 "The Digital Universe of Opportunities," IDC, April 2014

2013 and July 2014, Kaspersky reported 3.4 million malware detections on more than 1 million mobile devices. And if you consider that mobile attacks were up ten-fold, from 69,000 to 644,000 per month, the danger that accompanies cyber attacks is even more serious.

Mobile vulnerabilities are also emerging. For example, in June 2015 it was discovered that Samsung Galaxy smartphones were vulnerable to keyboard cracking. The weakness could give an attacker system-user privileges and let them steal contact information, text messages, login credentials and other valuable information. To be exact, the flaw affected as many as 600 million smartphones.

Tightening Regulations: In the face of data breaches, governments are ratcheting up their regulatory oversight of data privacy and holding businesses accountable for failing to protect the data they collect from customers. At least 75 countries currently have data protection laws, as do a select group of U.S. states such as California and Massachusetts. The harsh reality is that companies must now comply with both general and industry-specific regulations and guidelines, from Sarbanes-Oxley information Security Standards and Health Insurance Portability and Accountability Act (HIPAA) to Payment Card Industry Data Security Standard (PCI DSS).

This is just the tipping point – more are on the way. The Obama Administration's Consumer Privacy Bill of Rights, proposed in 2015, would require industries to establish codes of conduct around data and create privacy boards overseen by the U.S. Federal Trade Commission (FTC). Also in 2015, the European Union (EU) expects to complete an overhaul of its 1995 Data Protection Directive. This new regulation will strengthen citizen rights such as the so-called "right to be forgotten," or erased from data records.

A Time To Tap, A Time To Erase

Leveraging mobile data erasure to protect your corporate data is no easy feat. It can vary based on knowing exactly when mobile data must be expunged. To better understand this, we outline four key situations where mobile data erasure is absolutely necessary.

At Equipment End-of Life: When a mobile device is retired, it's either discarded or resold. For BYOD devices, in particular, that often involves returning the device to the equipment manufacturer's store. For corporate-owned mobile devices, that typically means sending the device to a recycler. In either case, any data contained within the device must be erased safely and permanently so that it can never reemerge, whether it's accidental or intentional.

When Equipment Is Serviced: If mobile equipment is serviced in-house, it remains in a secure environment, and there's no need to erase its data. But, and this is very important, if the device will be serviced by an external entity

Overwriting Requirements by Device Operating System

Not all mobile devices are created equal, especially when it comes to data erasure. Here's a high-level look at overwriting requirements by device.

Apple iOS: Because iPhone and iPad devices are encrypted by default, they don't require overwriting of all user data areas. Note, however, that the encryption key must be overwritten to make user data unreadable and the firmware should be updated.

Android: Android devices require overwriting of user data areas. A simple factory reset or reformat isn't 100% secure because data can easily be recovered after a reset.

BlackBerry: BlackBerry devices require the overwriting of user data areas and the removal of their IT policies.

Windows Mobile: Microsoft devices require overwriting of user data areas. A simple factory reset or reformat isn't 100% secure because data can easily be recovered after a reset.

Nokia Symbian: Nokia devices require overwriting of user data areas. A simple factory reset or reformat isn't 100% secure because data can easily be recovered after a reset.

6 "Mobile Cyber-Threats," Kaspersky Lab, October 2014

such as a mobile device manufacturer's retail store, you should be sure any and all sensitive data is removed before servicing takes place.

When Loaner Devices are Returned: Mobile users who have their equipment serviced at a repair center are often given loaner devices to use until their original devices have been fixed. If and when these loaner devices are used to access corporate systems, all of the files, texts, contact information, emails and media files should be erased before they're returned to the servicer.

When Equipment is Repurposed: When many corporate users replace their BYOD devices, they retain their old equipment or give it to their children or to other family members to use. Any corporate data that remains on those repurposed devices can easily become a liability and leave businesses vulnerable to a costly and dangerous security breach.

Certified Mobile Data Erasure is Fail-Safe

Many organizations have neglected to take advantage of mobile data erasure solutions because they assume factory resets or remote factory resets issued by mobile device management (MDM) will do the job. This is an oversight that can leave your data exposed.

First, it's important to understand that factory reset and data erasure are not the same. And mistaking one for the other is where many businesses go wrong. Factory reset simply removes pointers to the data, while leaving the data itself intact. The "deleted" data that remains on mobile devices—as well as on external SD cards—can quickly and easily be recovered using readily available software.

Second, mobile device management (MDM) software does not cover mobile data erasure. While MDM solutions typically offer security measures such as a firewall, encryption and virtual private network (VPN) support, its data deletion is limited to remote wipe. While "remote wipe" might sound like a fail-safe plan, it's not. The reality is that factory resetting simply removes pointers to the data, but it doesn't actually erase the data forever. And as researchers from Cambridge University recently discovered, the factory reset on Android devices are faulty and reversible. In fact, it's estimated that as many as 500 to 630 million Android devices might not be capable of completely wiping the data saved in their internal disks and SD cards. That means data can still be recovered. Without a USB connection to a computer running erasure software, which can detect all areas of the memory and initiate a full overwriting of the data, there will always be a possibility of recovery.

Likewise, mobile device manufacturers create apps that can overwrite a mobile device's data. While these apps can, in fact, erase data, they omit one very crucial element. And that's in the form of a tamper-proof report displaying electronic serial numbers and other details that prove, without a shadow of doubt, that all data has been expunged forever with no possible likelihood of resurfacing. They also are only capable of integrating with the operating system used by the manufacturer's device, and so they must be erased manually.

What organizations need, then, is an enterprise-class, certified mobile data erasure solution that truly protects their mission-critical data and mitigates the risk of data exposure. Look for a solution from a trusted provider that adheres to overwriting standards such as HMG Infosec and DoD 5220.22-M. The solution should also be approved as effective for sanitizing devices by an internationally recognized testing agency such as TÜV SÜD and DIPCOG.

It's also important to remember that after erasure, mobile devices are automatically reset back to their original operating systems and settings. So once erased, mobile devices can immediately be available for reuse by organizations.

In addition, an effective mobile data erasure solution should offer these three key characteristics.

Detailed Reporting: Not only must mobile data erasure software thoroughly overwrite mobile data, it must also generate a detailed, tamper-proof report as certified proof of the erasure. Verifiable reporting is the only way you can be certain mobile hardware has been sanitized before devices are discarded or recycled. It's also an essential part of regulatory and legal auditing requirements. Reporting should include relevant serial numbers and asset tags, software details for license harvesting, the condition of the hardware, as well as how and by whom the erasure was performed.

Broad Platform Support: Mobile data erasure software that's doing its job well should be able to communicate directly with all major mobile operating systems—including iOS, Android, BlackBerry, Windows Mobile and Nokia Symbian. It should also be able to detect and simultaneously erase data from a wide range of devices, regardless of the specific erasure requirements for each device. That will ensure that all your mobile devices are protected and it will accelerate the process of device sanitization.

Efficient, High-Volume Erasure: Finally, your chosen mobile data erasure solution should allow you to execute and automate erasure of multiple devices from a typical desktop computer or laptop. The automated erasure capability should be quick, easy to use and it should allow you to erase literally hundreds of mobile devices in a single day. The software should also send the erasure report to a central console to better streamline operational efficiencies, boost productivity and perform due diligence. For recyclers using multiple erasure units to enable the sanitizing of thousands of devices per day, the software should consolidate reports on a single console.

Final Thoughts

Mobile devices are transforming business with greater productivity and anywhere, anytime data access. They're also introducing heightened requirements for data protection. Mobile data erasure positions you to more effectively manage your mobile landscape, ensure compliance with multiplying government regulations, better protect customer information and intellectual property, and most importantly, mitigate the potential costs and legal consequences of data breaches. Best of all, it provides a fail-safe guarantee that your corporate and customer data doesn't leave your organization when your mobile devices leave.