blancco
technology group

WHITE PAPER

Why Data Erasure Should Be Part of Your Mobile Device Policy

With mobile devices, especially BYOD, flooding the workplace, organizations are scrambling to define rules for mobile device management. But many fail to include data erasure in their mobile device policy. It's a common mistake companies make and here's why it must change now.

In the spring of 2015, Tom Paterson's Nexus 5 smartphone stopped working. He took it back to the T-Mobile retail store, which mailed him a refurbished phone as a replacement. That's when things got interesting.

When Tom turned on the Nexus 5 smartphone, he discovered the personal information of the previous owner, including contact lists, a Facebook account and numerous apps. It turns out T-Mobile neglected to erase the original owner's data on the refurbished phone before it was reissued to someone else. For its oversight, the company ended up becoming the subject of a less than flattering story in the *New York Times*.[1]

This won't be the last time an event of this nature makes headlines, and not in a good way. But it's the kind of incident CIOs and other executives are increasingly concerned with preventing from happening - and that's rightfully so. It's especially true when you consider that BYOD has shifted from an occasional occurrence to the 'new normal.'

To protect themselves, enterprise businesses need a detailed and documented policy for how they'll manage mobile devices and safeguard mobile data. And a key part of that policy should cover data erasure at critical transition points in the life cycle of each device.

1.6 billion

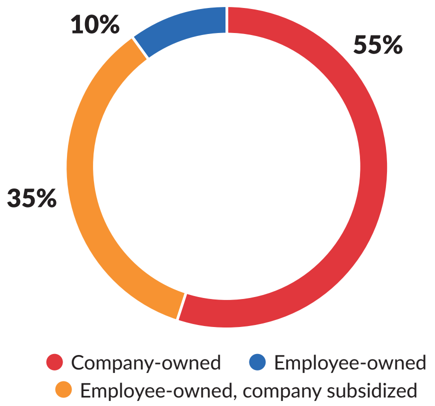
BYOD devices projected to be in use in 2014

More Devices, More Data

There's no denying that smartphone and tablet use in the workplace has exploded. And a growing proportion of that equipment is BYOD. In fact, 1.6 billion BYOD devices were projected to be in use by 2014, according to Gartner.[2] Now consider this: Nearly half of mobile devices in the workplace are now employee-owned, according to Spiceworks.[3] (See Figure 1.) And as Gartner reveals, 70 percent of professionals will perform work-related activities on a personal device by 2018.[4]

70%

Professionals will perform work-related activities on a personal device by 2018



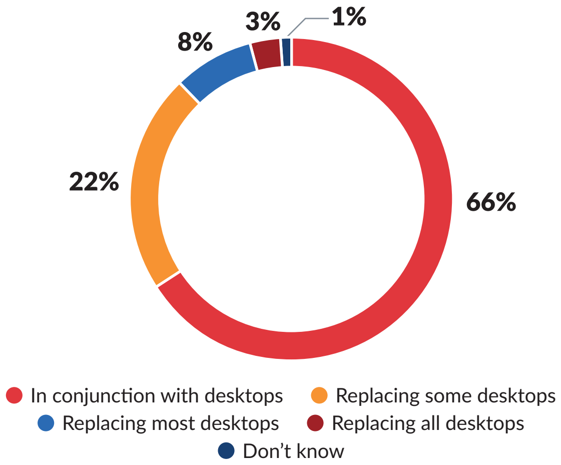
Source: Spiceworks, October 2014

Nearly one-half of mobile devices in the workplace are employee-owned.

Figure 1: Mobile Device Ownership in the Workplace

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

[1] "The Replacement Cellphone With a Past Life," The New York Times, June 20, 2015
[2] "Bring Your Own Device: The Facts and the Future," Gartner, May 2013
[3] "The Rise of the Mobile Empire," Spiceworks, April 2015
[4] "Bring Your Own Device: The Facts and the Future," Gartner, May 2013

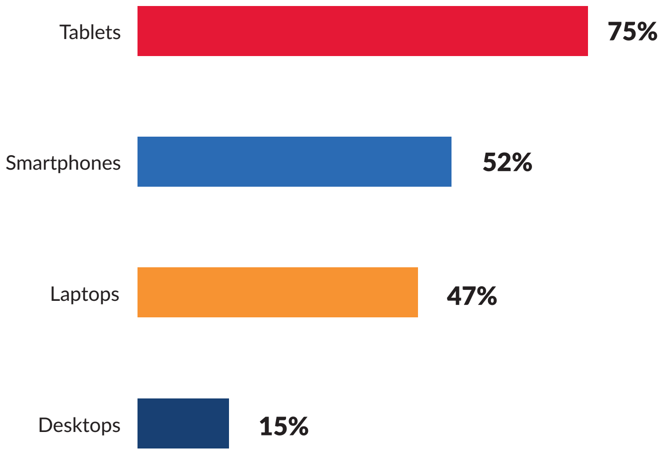


Source: Spiceworks, October 2014

While two-thirds of mobile devices are used in conjunction with desktops, nearly one-third have replaced some if not most desktops.

Figure 2: How Mobile Devices Are Used

At the same time, your organization's data stores are only growing. The global volume of data will mushroom from 4.4 zettabytes (ZB) in 2013 to 44 ZB in 2020, predicts IDC.[5] And the reality is that more of that data, from employee records to customer information to intellectual property, is ending up on mobile devices. After all, mobile devices are just computers with a small screen. To put this into context, the average smartphone has more power than the processors that landed Apollo 11 on the moon. In fact, many tablets can store 128 GB of data, including customer names, emails, usernames and passwords, photos and much more.



Source: Spiceworks, October 2014

Use of desktops will increase 15 percent in the next three years, but use of tablets will leap 75 percent.

Figure 3: Increase in Device Use in Next Three Years

As your enterprise manages more data, government agencies around the world are simultaneously drafting new and more stringent data protection laws. Just how important is legislation? At least 75 countries have data protection laws on the books, as do U.S. states such as California and Massachusetts. Companies must also comply with both general and industry-specific regulations and guidelines, from the Sarbanes-Oxley information security standards and the Health Insurance Portability and Accountability Act (HIPAA), to the Payment Card Industry Data Security Standard (PCI DSS).

But that's just the tip of the iceberg; more legislation is on the way. For one, 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. The new regulation is expected to strengthen citizen rights such as the "right to be forgotten", or erased from data records.

All of these factors—more devices, more data and more regulations—reinforce just how critical it is to establish a robust policy to govern the use of mobile information. That policy must include provisions for how data will be erased at critical transition points.

120 million

The market for refurbished mobile phones will nearly double to 120 million units in 2017

Why? Let's put it this way, devices are frequently lost and stolen. When they reach end-of-life, they might be passed on by the company to other employees or passed on by the employee to a family member. Increasingly, devices find new life in the second-hand market. In fact, Gartner predicts that the volume of refurbished mobile phones will nearly double from 56 million units in 2014 to 120 million units in 2017.[6]

[5] "The Digital Universe of Opportunities," IDC, April 2014
[6] "Reused, Resold, Recycled — Where Do Old Smartphones Go?", Gartner, February 2018

That's why it's imperative for you make sure any sensitive corporate data is verifiably removed from your organization's devices, or you could suffer a data breach that could have serious negative consequences, including financial losses, damaged brand reputation and even endangering the lives of employees.

The Data is in the Details

Development of a mobile device policy should include input from stakeholders across the enterprise. While ownership and management may reside with the CIO and data security team, the Legal function and Governance, Risk and Compliance function should also have input. These constituencies should contribute to initial development of the policy as well as ongoing updates as business, regulatory and data security needs change.

Your mobile policy must also be distributed throughout the organization and for that reason your HR and Corporate Communications functions should be involved. New hires should be educated on the policy and on their responsibilities for following it, and existing employees should receive reminders on an ongoing basis.

A robust mobile device policy should include the following considerations:

Devices: Start by determining how closely you want to limit the endpoints in your organization. You might issue only one type of device to employees. Or you might allow employees to select from a range of company-approved devices. Or you might allow workers to bring their own device.

Encryption: Whether you take a company-issued or BYOD approach, make sure all corporate data on all devices is encrypted. Apple's iOS encrypts data by default. Otherwise, you'll need to add or enable encryption software. Also consider containerization, such as the Samsung Knox solution, which keeps personal data in one area of the device and corporate data in another.

Apps: Software used for business, such as email, browser, VPN apps, file sharing cloud services, marketing automation solutions like Salesforce and so on, needs to be secure. Set rules for which apps can be used for business and which cannot. Then ensure that every device in your enterprise is configured properly.

Protection: Establish clear rules for obvious security measures, such as password protecting devices and requiring strong passwords for network login. Also be sure your company's security software, such as antivirus, extends to mobile devices.

Behavior: Set rules for employee behaviors that can mitigate the risk of data exposures. Specify which corporate data can be accessed from the device and which corporate data can be stored on the device. Offer guidance on how employees can avoid device theft and what steps they should take if a device is lost or stolen.

Data Erasure: Finally, include in your policy clear guidelines for what happens to mobile data when devices reach end-of-life. Specifically, you need to ensure that all data is thoroughly and verifiably removed from the device before it's reused, resold or disposed of. Specify the data erasure solution that will be used, as well as each step in the erasure process. Include roles and responsibilities, such as what employees must do before a device is retired, sent for repair or handed down to the next employee and what steps IT or data security staff must take. Don't neglect scenarios such as how data will be erased in the event of an employee termination.

Know When to Go

Fundamental to effective data erasure is knowing how and when to erase data. Many organizations assume factory resets or mobile device management (MDM) will do the job. This is an oversight that can leave your data exposed.

First, factory reset does not equal data erasure. Factory reset simply removes pointers to the data, while leaving the data itself intact. The "deleted" data from mobile devices, as well as on external SD cards, can quickly and easily be recovered using readily available software.

Second, MDM software does not cover mobile data erasure. While MDM typically offers 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 data destruction, it's merely a factory reset that doesn't truly expunge the data.

Likewise, there are apps available on various App Stores that can overwrite a mobile device's data. While these apps can in fact erase data, they omit a crucial element, which is a verifiable report with electronic serial numbers and other details that can prove the data has been expunged. They also work only with the operating system used by the manufacturer's device and they must be downloaded to each device one by one and executed manually.

Protecting mobile data also means knowing exactly when that data must be expunged. To help, we've outlined four key situations where mobile data erasure is necessary.

At Equipment End-of-Life: When a mobile device is retired, it's either repurposed, discarded or resold. For BYOD devices, that often involves returning the device to the store. For corporate-owned devices, that typically means sending the device to a recycler. In any case, all data the device contains must be erased so that it doesn't fall into the wrong hands.

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 if the device will be serviced by an external entity such as a mobile-device store, you should be sure any 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. If these devices are used to access corporate systems, they 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 the device is vulnerable and should be erased.

Overwriting Requirements by Device

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

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

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

Mobile Data Erasure You Can Count On

The data erasure aspects of your mobile device policy are only as effective as the data erasure itself. To truly protect your mission-critical data and mitigate the risk of data exposure, you need an enterprise-class, certified mobile data erasure solution. 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 or DIPCOG.

In addition, an effective mobile data erasure solution should offer the following three key characteristics:

Detailed Reporting: Not only must mobile data erasure software thoroughly overwrite mobile data; it must also generate a detailed report as 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 IMEI numbers, serial numbers, the device model and the condition of the hardware, and how and by whom the erasure was performed.

Broad Platform Support: Good mobile data erasure software 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 mobile data erasure solution should allow you to execute and automate erasure of multiple devices from a typical desktop computer. The automated erasure capability should be quick and 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 or cloud for efficiency and easy access. 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.

More employees are using mobile devices and more of those devices are BYOD. Meanwhile, your organization is managing more data and facing more threats of data exposure. A detailed, documented mobile device policy can go a long way toward strengthening your data security profile. And with effective, verifiable mobile data erasure as part of that policy, you can be certain your enterprise is leveraging mobile technology to perform more effectively while safeguarding your mission-critical information assets.

ABOUT BLANCCO TECHNOLOGY GROUP

Blancco Technology Group is a leading, global provider of mobile device diagnostics and secure data erasure solutions. We help our clients' customers test, diagnose, repair and repurpose IT devices with the most proven and certified software. Our clientele consists of equipment manufacturers, mobile network operators, retailers, financial institutions, healthcare providers and government organizations worldwide. The company is headquartered in Alpharetta, GA, United States, with a distributed workforce and customer base across the globe.

Blancco, a division of Blancco Technology Group, is the global de facto standard in certified data erasure. We provide thousands of organizations with an absolute line of defense against costly security breaches, as well as verification of regulatory compliance through a 100% tamper-proof audit trail.

SmartChk, a division of Blancco Technology Group, is a global innovator in mobile asset diagnostics and business intelligence. We partner with our customers to improve their customers' experience by providing seamless solutions to test, diagnose and repair mobile assets. SmartChk provides world-class support, pre and post implementation, allowing our customers to derive measurable business results.

CONTACT US

For Sales & Marketing, Please Contact:
Email: marketing@blancco.com

For Corporate Communications & PR, Please Contact:
Email: press@blanccotechgroup.com