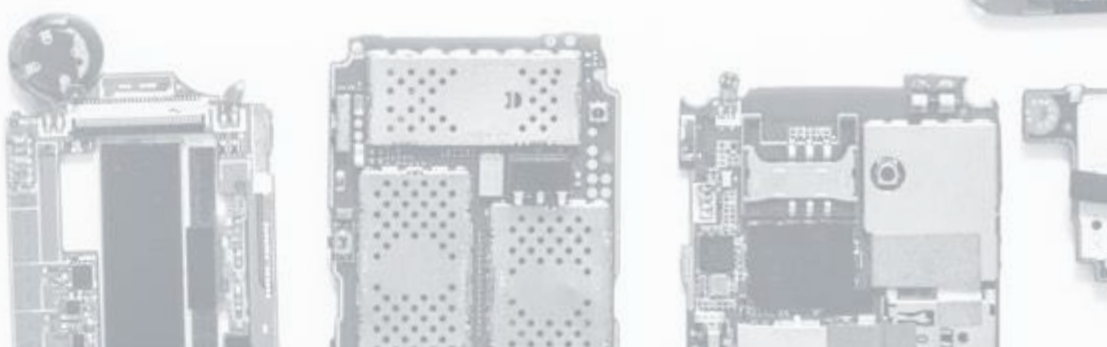
blancco

TREND REPORT: Q4 2017

# State of Mobile Device Repair & Security



February 2018

# Table of Contents


**Introduction** 3

**About the Data Powering the Report** 3

**Key Trends & Insights** 4

- Older Android Versions Are Sticking Around, While iOS Users are Quick to Update 4
- Majority Using Secure Erasure Methods to Address iOS & Android Devices 7
- Failure Rates Similar for Android & iOS Overall, but Vary Significantly by Region 8
- Failure Rates for iOS: iPhone 6 & 6S Continue to Disappoint 9
- Failure Rates for Android: Samsung Models Stand Out as Problematic, but are Getting Better 9
- Androids & iOS Share Headset Issues; Other Problems Vary 11
- Diagnostics Tests: Average of 15 Tests Performed for iOS & Android Models Worldwide 11

**Conclusion** 14

**About Blancco** 15

# Introduction

The global market for used smartphones will be worth about $30 billion in 2020, with an average selling price of $136 per device, according to IDC. And with so many phones making their way through mobile warehouses and processing centers, security and processing efficiency are key, we've compiled research to highlight best practices for mobile security and share information that could optimize warehouse operations for mobile diagnostics and erasure moving forward. In this report, we'll be focusing solely on iOS and Android operating systems, as they now make up over 99 percent of all current smartphone sales. However, keep in mind that Blackberry and Windows Phone models should be considered in any mobile diagnostics or erasure solution in which you choose to invest.

# About the Data Powering the Report

The Mobile Device Repair & Security Report is the first of its kind. Following the success of our quarterly Mobile Device Performance & Health reports, this new report focuses less on topics that are important to consumers and more on issues that affect mobile processing centers, repair centers and resellers.

This quarterly review of global mobile device trends includes information related to: erasure standards used to wipe devices, time spent on erasure, types of mobile diagnostics tests performed across different operating systems, performance issues and model-specific failure rates.

The information contained in this report is based on internal mobile diagnostics and mobile erasure data collected from iOS and Android mobile devices that were brought into hundreds of mobile carriers and device manufacturers for diagnostics tests and mobile erasure in North America, Europe, Asia and Australia from October 1, 2017 to December 31, 2017. Diagnostics tests and erasure were performed using the Blancco Mobile Diagnostics platform and Blancco Mobile Device Erasure software, and the reports were stored on the Blancco Management Console. Mobile organizations can leverage this information to ensure a better customer experience and improve their response to mobile security best practices.

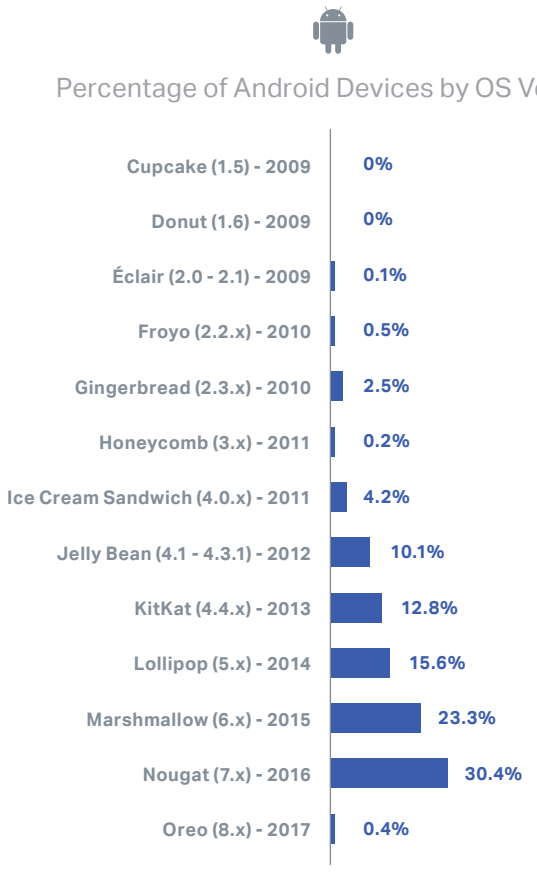
Read on to see the following highlights:

- Older Android Versions Are Sticking Around, While iOS Users are Quick to Update
- Majority Using Secure Erasure Methods to Address iOS & Android Devices
- Failure Rates Similar for Android & iOS Overall, but Vary Significantly by Region
- Failure Rates for iOS: iPhone 6 & 6S Continue to Disappoint
- Failure Rates for Android: Samsung Models Stand Out as Problematic, but are Getting Better
- Androids & iOS Share Headset Issues; Other Problems Vary
- Diagnostics Tests: Average of 15 Tests Performed 11 for iOS & Android Models Worldwide

## Older Android Versions Are Sticking Around, While iOS Users are Quick to Update

Approximately 30.5 percent of Android devices that underwent the Blancco mobile device erasure process in Q4 2017 were running Android versions from 2013 or earlier, with a couple of instances as far back as Cupcake (1.5) and Donut (1.6) (both from 2009) creeping in. This goes to show that mobile processors must be prepared to address devices long after they first hit the market—even up to a decade later. To do this, you'll need to rely on erasure software that can work across any mobile device, no matter its age, software or model type. Here are the percentages for each version of Android addressed during our erasure process:

*Figure 1.*



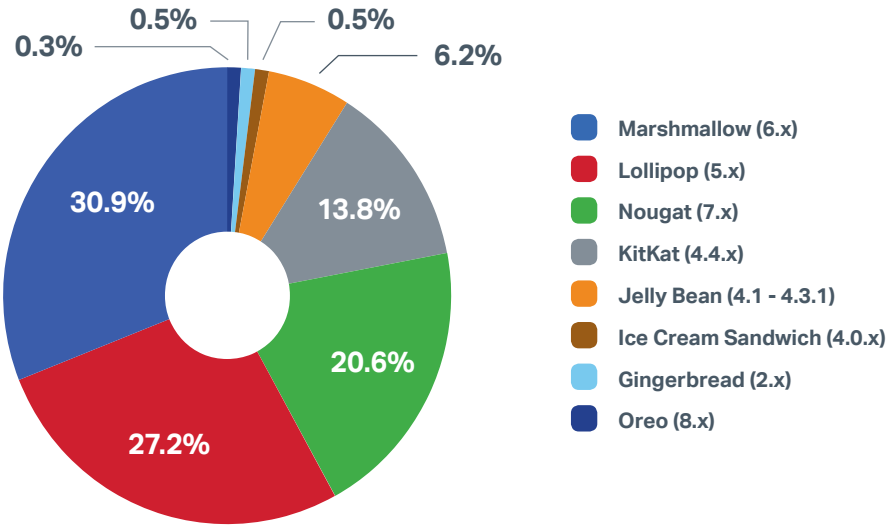

***Note: Numbers throughout the report may not add up to 100%, due to rounding and the fact that only the top three global focus areas have been included in the final report.***

Android models running version 6 and above are encrypted by default like iOS devices; however, any models before Marshmallow are not encrypted by default and are therefore at risk if only a reset is performed. Research shows that fewer than 1 percent (or slightly over, depending on the source) of Android phones on the market are running Oreo, the latest version of Android software (version 8). Android fragmentation has always been an issue, and it's not getting any clearer. With so many different types of devices running Android software, it's difficult to formulate security best practices or performance fixes across the board. And because users are having trouble updating

to the latest software releases, or even having awareness of when they hit the market, this issue is further compounded. Over half of all Android devices are more than two years out of date with their software updates, according to tech expert Dan Luu's analysis. Here's what those numbers look like in the mobile industry overall as of November 9, 2017, during the timespan this report covers.

Android OS Distribution

*As of November 9, 2017*




*Source: Android Developers, 2017*

# Key Trends & Insights

According to the latest data (as of February 2018) from the Android Developer Platform, these numbers have shifted slightly, but they're still very similar. Here's what they currently look like. You can see some of the newer versions are starting to make small gains:

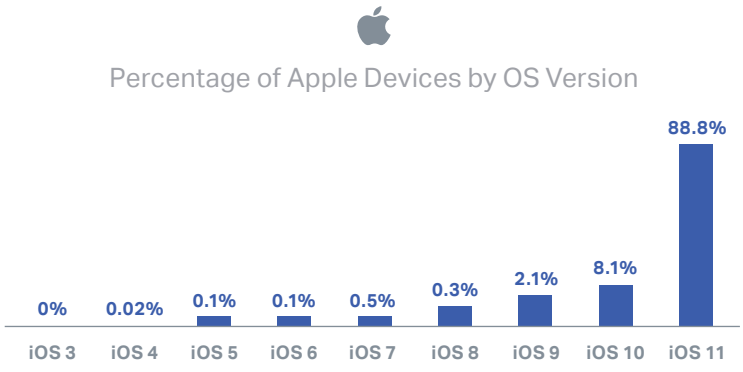
| VERSION | CODENAME | API | DISTRIBUTION |
|---|---|---|---|
| 2.3.3 - 2.3.7 | Gingerbread | 10 | 0.3% |
| 4.0.3 - 4.0.4 | Ice Cream Sandwich | 15 | 0.4% |
| 4.1.x | Jelly Bean | 16 | 1.7% |
| 4.2.x | | 17 | 2.6% |
| 4.3 | | 18 | 0.7% |
| 4.4 | KitKat | 19 | 12.0% |
| 5.0 | Lollipop | 21 | 5.4% |
| 5.1 | | 22 | 19.2% |
| 6.0 | Marshmallow | 23 | 28.1% |
| 7.0 | Nougat | 24 | 22.3% |
| 7.1 | | 25 | 6.2% |
| 8.0 | Oreo | 26 | 0.8% |
| 8.1 | | 27 | 0.3% |

*Data collected during a 7-day period ending February 5, 2018. Any versions with less than 0.1% are not shown.*

Based on this data, Android devices will require secure erasure with software-based overwriting to comprehensively remove data for at least the next several years. A simple reset is not enough to address lingering personal data because encryption is not included as standard in Android versions prior to Marshmallow (6). It's best practice to use overwriting across the board when it comes to Android.

iOS models are a different story. All iOS models are encrypted by design in iOS 8 and above, and most of the models wiped during this testing period (88.8 percent) were running iOS 11. This latest version of Apple software was released on September 19, 2017 and is compatible with the following phone models: Phone 5S, 6, 6 Plus, 6S, 6S Plus, SE, 7, 7 Plus, 8, 8 Plus and iPhone X. In short, most Apple users are up-to-date on the latest software, while most Android users are not.

*Figure 3.*



## Majority Using Secure Erasure Methods to Address iOS & Android Devices

To address the different erasure needs required by various Android devices, our data shows that most Blancco customers are using secure, software-based overwriting to erase their sensitive data. Only 2.4 percent of devices used Android Smart Reset (which includes encryption and a factory reset), and 1.8 percent of devices were wiped via a Factory Reset (which, as we discussed, is more secure for more recent devices). Most customers, however, used Aperiodic random overwrite (67.2 percent) and HMG Infosec Standard 5, Lower Standard (25.5 percent).

These overwriting methods ensure that sensitive data is completely removed from Android devices. This type of comprehensive erasure provides important peace of mind for customers selling and purchasing used phones.

*Figure 4.*

Erasure Method Choices by Android OS

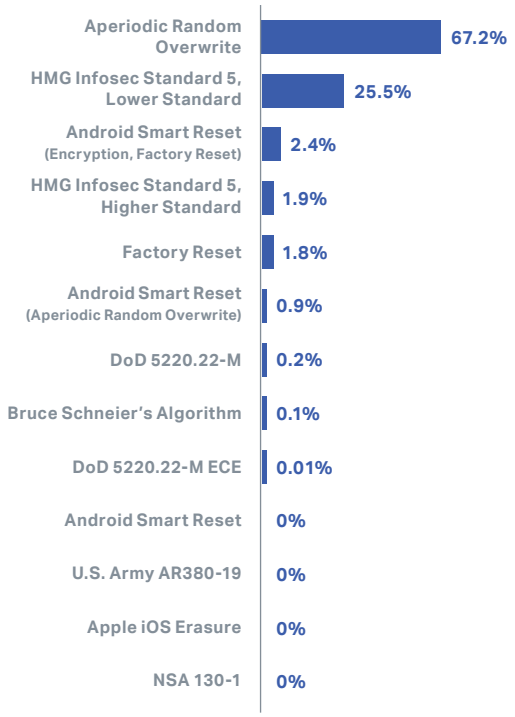
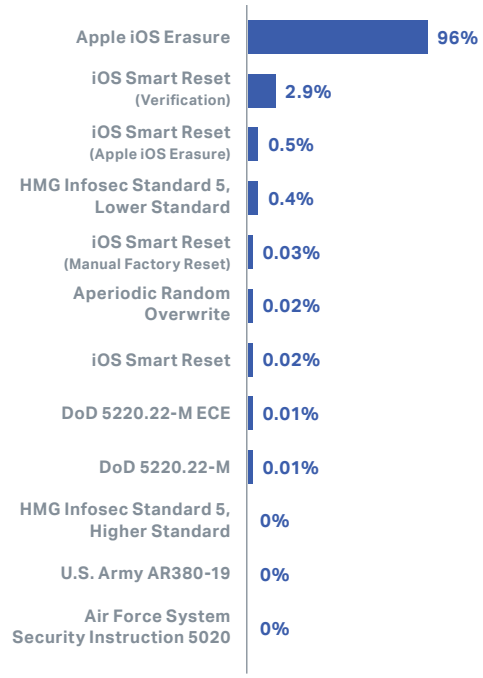



*Figure 5.*

Erasure Method Choices by Apple OS




Our data indicates that the majority of iOS devices (96 percent) were erased using Apple iOS erasure, which is extremely secure on recent iPhone models that are encrypted by default. Blancco software supports iOS erasure, as well as iOS Smart Reset (Verification), iOS Smart Reset (Manual Factory Reset) and all other erasure standards for iOS devices. Depending on the industries you're selling devices into or erasing devices for, you may choose to use other erasure methods listed below, such as DoD or U.S. Army. When dealing directly with consumers, Apple iOS erasure should work just fine for models running recent software.

## Failure Rates Similar for Android & iOS Overall, but Vary Significantly by Region

Across our three major global markets: Asia, North America and Europe, failure rates (or the number of mobile phones that showed some sort of diagnostics issue during testing) were similar for Androids and iPhones overall, at 12.5 percent for iOS and a slightly higher percentage for Android, at 14 percent.

However, these rates do vary significantly across regions. While the iOS failure rate in North America was only 12 percent, Europe and Asia had much higher numbers, as you can see from the chart below. The same applies for Android. While the failure rate in North America was only 9 percent, it was a shocking 40 percent in Europe and 21 percent in Asia. This huge disparity could be caused by the number of devices brought into our testing centers and the reasons they were brought in (expected diagnostics issues vs. simple checks, for example). We find that Europe tends to deal a lot with older Android devices that have always had issues, while US-based consumers switch to newer models more quickly and, U.S. mobile processors encounter fewer issues.

*Figure 6.*

iOS Device Failure Rates, Q4 2017

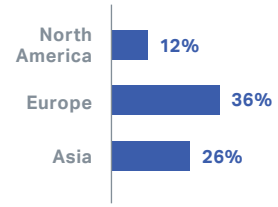
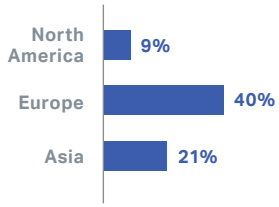



*Figure 7.*

Android Device Failure Rates, Q4 2017



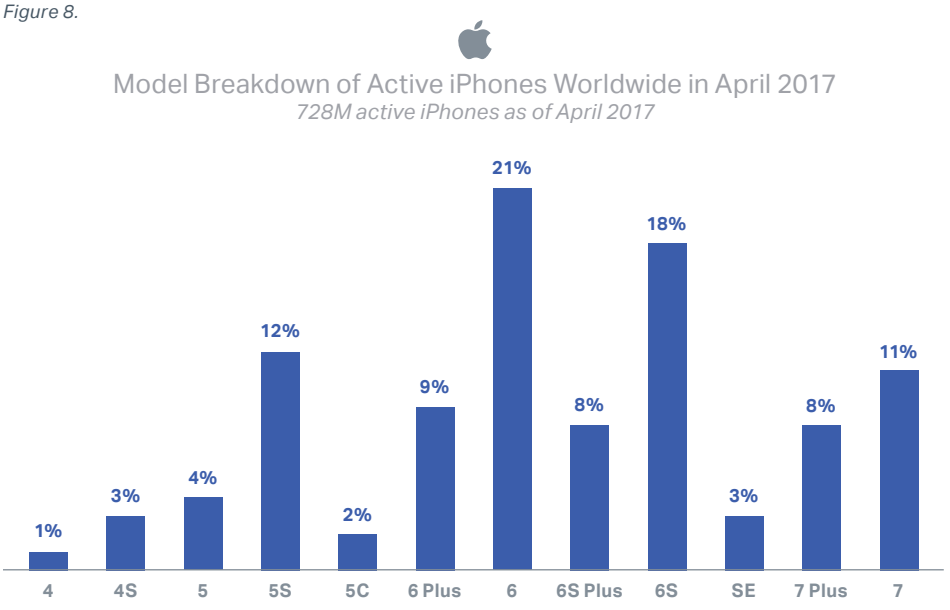

Top 10 iOS Failure Rates by Model, Q4 2017

| MANUFACTURER | MODEL | FAILURE RATE % |
|---|---|---|
| Apple | iPhone 6 | 26% |
| Apple | iPhone 6S | 14% |
| Apple | iPhone 6S Plus | 9% |
| Apple | iPhone 7 Plus | 9% |
| Apple | iPhone 6 Plus | 9% |
| Apple | iPhone 7 | 8% |
| Apple | iPhone 5s | 6% |
| Apple | iPhone SE | 6% |
| Apple | iPhone 8 Plus | 2% |
| Apple | iPhone 5 | 2% |

## Failure Rates for iOS: iPhone 6 & 6S Continue to Disappoint

Following the trends covered in our Q3 State of Mobile Performance & Health Report, the iPhone 6 and 6S continue to lead the pack in terms of failure rates, with a 26 percent failure rate for iPhone 6 devices and a 14 percent failure rate for iPhone 6S devices. This could partially be because Apple 6 models were the most popular on the market in the latter half of 2017. See the graph from Statista below.

*Figure 8.*




*Source: Newzoo / Statista*

However, if Apple's online forums and thousands of articles online are to be believed, the iPhone 6 models truly do have more hardware issues than most other mobile devices. In Q3 2017, the iPhone 6 and iPhone 6S had failure rates at 26 percent and 11 percent, respectively, so the 6 model has stayed about the same, while failures for the 6S have increased by 3 percent. In 2018, we can expect to see the newest iOS models, the iPhone 8 and iPhone X, start to populate this list. Currently, there is not enough information to determine what their failure rates will look like, but we expect the iPhone 6 will continue to stay in the top spot for at least the next quarter or two.

## Failure Rates for Android: Samsung Models Stand Out as Problematic, but are Getting Better

In terms of Android failure rate by manufacturer, Samsung models had the highest diagnostics failure rates by far at nearly 34 percent. While this seems like bad news for the brand, it's a sharp decrease from the failure rates reported in our previous reports, which showed a failure rate of 61 percent in Q2 2017 and 53 percent in Q3 2017. In second place this quarter was Xiaomi at 13 percent, followed by Motorola at nearly 9 percent. 5 out of the top 10 models by failure rates were Samsung models, while

Xiaomi was second with two of the top worst performing models. Th Xiaomi Redmi 4 was the top worst-performing Android model, with a failure rate of nearly 9 percent. Compare this to the failure rate of the iPhone 6, with a failure rate of 26 percent. That's a significant difference that must be noted by any mobile reseller or support center. (In other words, keep a close eye on any iPhone 6 models that come in!)

*Figure 9.*

Top 10 Android Manufacturers by Failure Rate, Q4 2017

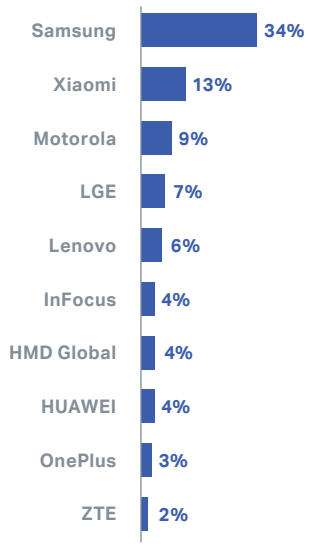
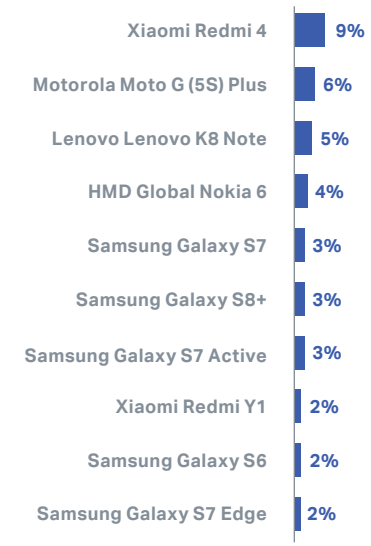



*Figure 10.*

Top 10 Android Models by Failure Rate, Q4 2017




## Androids & iOS Share Headset Issues; Other Problems Vary

When considering the top diagnostics issues encountered by both Android and iOS devices, headset issues were on the top 5 list for both, but other issues differed. Bluetooth issues were the top reported problem with iOS devices, while Android devices reportedly had significant performance issues (speed, battery life, frozen screen, etc.).

Updating to the latest Android software releases can help customers avoid some of these performance issues, as can shutting down extra apps that are running in the background, clearing their app caches and disabling widgets.

*Figure 11.*

Top 5 iOS Performance Issues Worldwide, Q4 2017

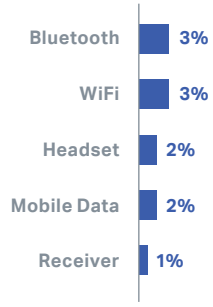
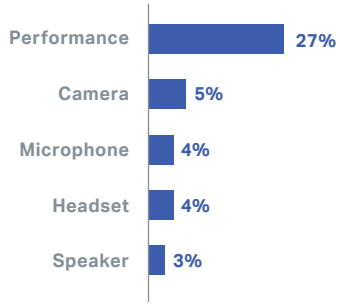



*Figure 12.*

Top 5 Android Performance Issues Worldwide, Q4 2017

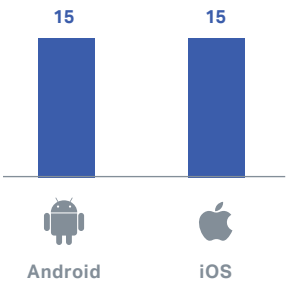



## Diagnostics Tests: Number Performed & Global Results

Our Q3 Mobile Diagnostics Data Shows that our global customers typically ran around 15 diagnostics tests per model on both Android and iOS devices, despite the fact that 40+ tests are available from the Blancco Diagnostics product offering.

*Figure 13.*

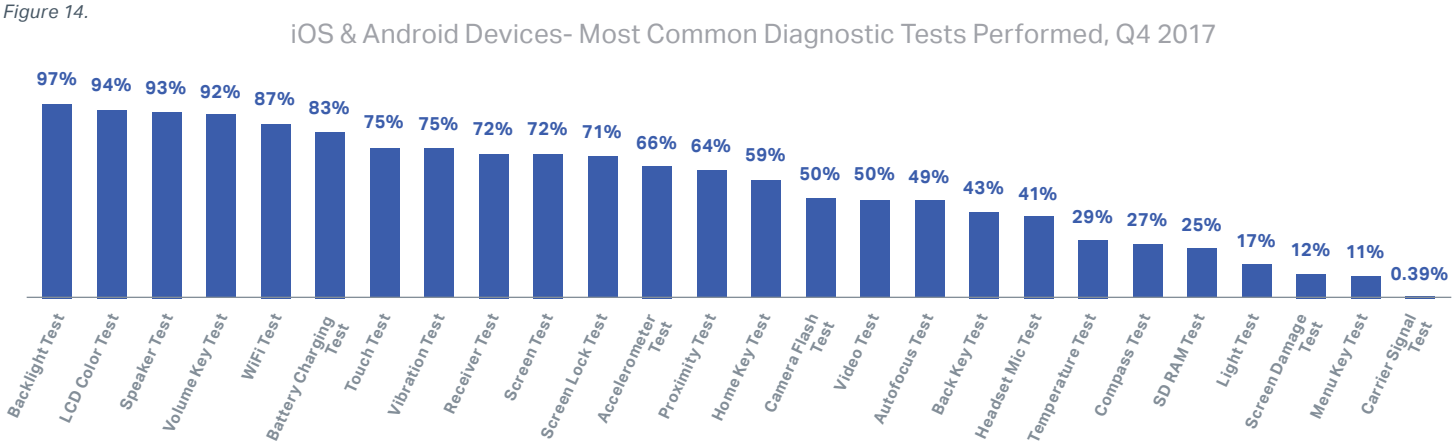
Average Number of Diagnostic Tests Performed Globally



# Key Trends & Insights

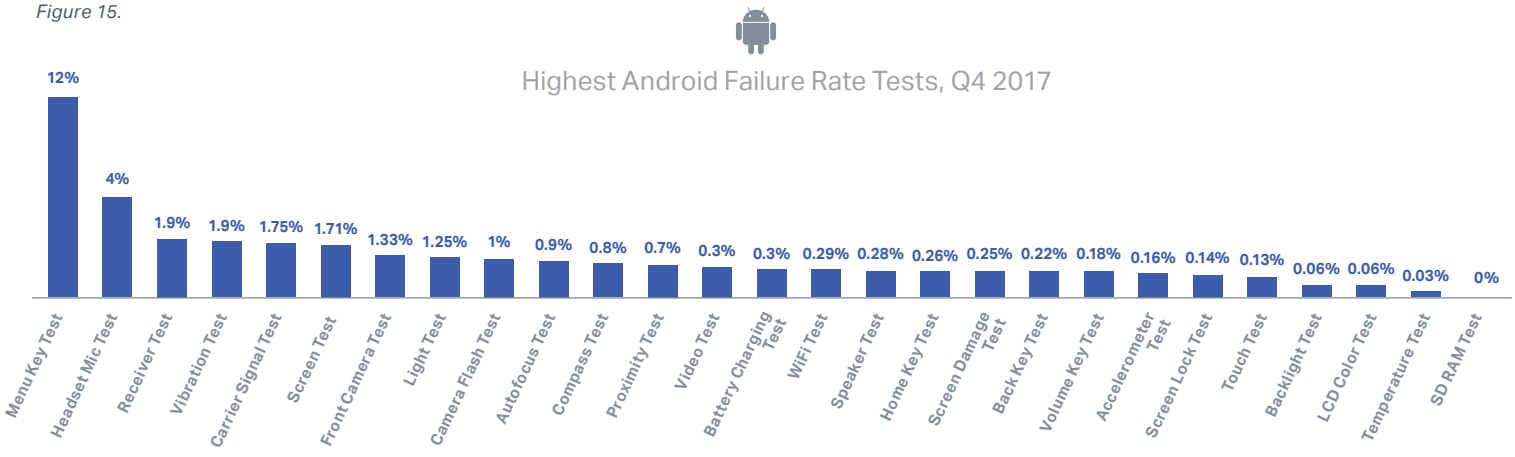
The following chart shows the most common diagnostics tests performed on iOS and Android devices. As you can see, backlight, LCD color and speaker tests took the top three spots. Take a look at the most common tests below and compare the diagnostics tests you're running within your mobile organization.

*Figure 14.*




Within these tests, we also gathered data around the highest diagnostics failure rates for each test by operating system. Android, shown below, had the highest percentage of diagnostics failures for the "Menu Key Test," at 12 percent failure rate. The second highest failure rate was the Headset Mic Test, at about four percent. This would indicate that Android models have a significant amount of issues with their Menu Keys.

*Figure 15.*

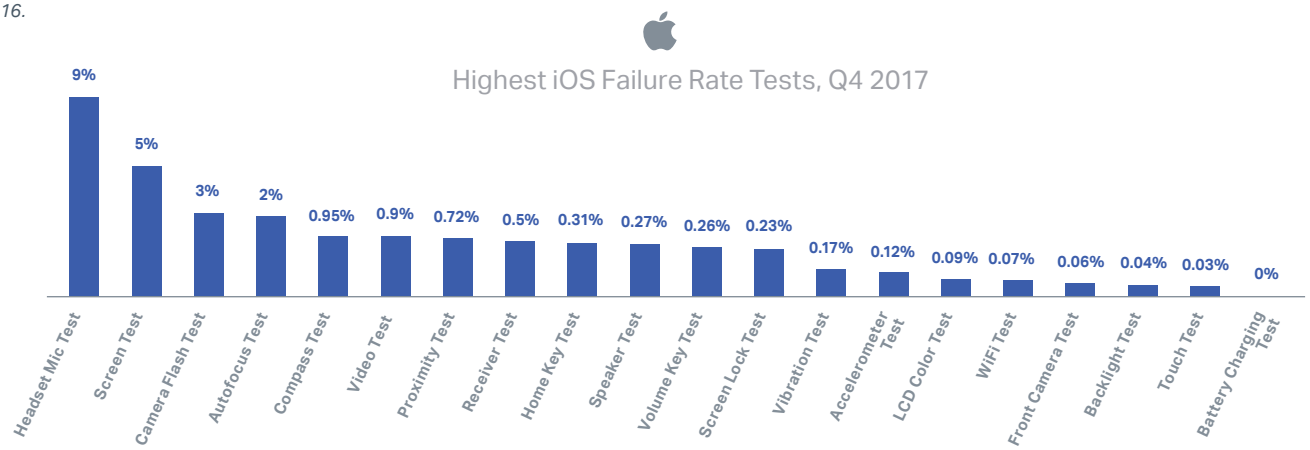





blancco

Below is the iOS testing chart. As you can see, the headset mic test was the most likely to fail for iOS (9 percent), whereas it was listed as the number two issue for Android devices. In addition to headset mic issues, iOS devices were most likely to fail their screen tests (5 percent) and camera flash tests (3 percent). When processing these devices, be sure to keep these issues top of mind.

*Figure 16.*




# Conclusion

Through data collected from iOS and Android devices brought into wireless carriers and device manufacturers for Blancco testing and erasure, we have learned that older Android models and software versions continue to flood the market, making it more important than ever to ensure data is securely erased before resale or recycling. We've also learned that Samsung models continue to have the highest failure rate for Android phones, while the iPhone 6 is the most troublesome for iOS. Finally, we've learned that failure rates for iOS and Android vary significantly by region and that Android phones suffer with performance-related issues such as high CPU, RAM and memory consumption, outdated software versions and misbehaving apps.

In today's highly competitive marketplace, mobile resellers, warehouses and mobile call centers must deliver maximum value for their customers across every channel– with the goal of optimizing the long-term performance of mobile devices, increasing mobile resell values, reducing customer complaints and number of returned devices and decreasing time spent diagnosing and erasing devices.

The key to achieving these goals is being able to diagnose, erase/wipe and repair device issues quickly, easily and accurately. With Blancco Mobile Device Eraser and Mobile Diagnostics solutions, you can accomplish these goals, while also creating efficiencies across your diagnostics and erasure processes. For more information about how we can help you meet your organization's unique needs, contact us today for a free strategy session and trial.

# About Blancco

Blancco is the de facto standard in data erasure and mobile device diagnostics. The Blancco Data Eraser solutions 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. Our data erasure solutions have been tested, certified, approved and recommended by 18 governing bodies around the world. No other security firm can boast this level of compliance with the most rigorous requirements set by government agencies, legal authorities and independent testing laboratories.

The Blancco Mobile Diagnostics solutions enable mobile network operators, retailers and insurers to easily, quickly and accurately identify and resolve performance issues on their customers' mobile devices. As a result, mobile service providers can spend less time dealing with technical issues and, in turn, reduce the quantity of NTF returns, save on operational costs and increase customer satisfaction.

For more information, visit our website at www.blancco.com.

# Contact Us

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

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