wandera

# Uncovering the true costs of Enterprise Mobility

## A study into the total cost of ownership

Mobile devices are everywhere and we all use them to improve communication, but how much do they really cost your enterprise? A common misconception is that total cost of ownership is neatly captured within the simple equation, “device + carrier cost.” But the true cost is so much more.

## Table of Contents

## Executive Summary

Enterprise mobility is an inevitable cost of doing business. Devices and connectivity are as fundamental to your operations as the employees themselves.

The Total Cost of Ownership (TCO) of enterprise mobility is made up of a number of factors, some of which can be excessively expensive or unnecessary altogether. Are enterprises examining enough of these factors to calculate an accurate TCO, and in turn considering all the measures that can reduce costs and mitigate risks?

Typical perceptions of TCO are a simple equation of the 'Device + Plan'. This is grossly inadequate, made worse when "Plan" only includes predicted carrier costs, not unexpected extras such as roaming bill shocks or excessive data usage.

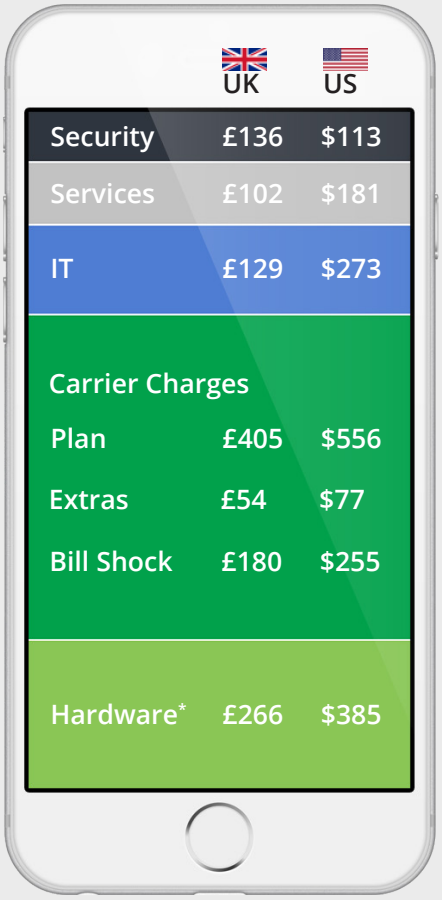
Assuming that the TCO is made up of just the device and the plan will lead to expectations that TCO is in the region of $853 per device per annum (£628 in the UK). But this report shows that in reality, the actual TCO is closer to $1,840 (£1,272 in the UK).

This actual TCO figure includes cost factors that are too often forgotten: the IT resources required to manage the devices; the services that may be deployed to assist with their management e.g. Enterprise Mobility Management (EMM) and Telecom Expense Management (TEM); mobile security software; and the cost of remedying mobile security breaches.

Disregarding these factors leads to an underestimated TCO and complacency in regards to mobile security, legal and financial risks.

**Key Findings:**

- In the US the actual TCO per device is $1,840 - 116% more than commonly expected - which equates to $51.9 billion in total spend for American businesses*
- In the UK the actual TCO per device is £1,272 - 103% more than commonly expected - which equates to £4.4 billion in total spend for UK companies*
- $987 (£644 in the UK) of costs including services, security and IT are not being taken into account when calculating the TCO of enterprise mobility
- On average $407 in the US or £352 in the UK could be saved per device annually through appropriate mobile control - which adds up to millions for large companies.
- Total cost savings of $11.5 billion are available in the US and £3.7 billion in the UK*
- Globally, companies spend twice as much on cleaning up mobile security breaches than on mobile security software
- 28% of US companies report having suffered a mobile breach in the last 12 months – with the cost of remedying the breach at $250,000 to $400,000 in many cases
- 18% of UK companies report having suffered a mobile breach in the last 12 months – with the cost of remedying the breach at £100,000 to £250,000 in many cases
- 'Bill shocks' from unexpected carrier charges are the second greatest single contributor to overall TCO for the largest companies globally - 14% of the TCO




**Total US $1,840**
**Total UK £1,272**

*Where devices are refreshed every 2 years costs have been annualized. Where carrier contracts include free devices these costs have been seperated out.*
**Wandera research: The total number of corporate liable devices is estimated to be 28.2 million in the US, and 10.4 million in the UK*

With the evidence that an enterprise's TCO for mobility is higher than many would expect, comes the revelation that, depending on company size, **45% - 65% of the entire cost is controllable**. The controllable elements are essentially the carrier costs and security spend. The other categories of hardware cost, IT spend and management platforms are largely inevitable.

The controllable cost areas can each be reduced by significant proportions. A successful data cost management policy can reduce each element of the carrier costs: carrier plans by 10%, carrier extras by 50% and can even remove bill shock costs altogether. Similarly, improved security measures such as mobile threat prevention software can remove the need for mobile security breach remedy altogether, reducing the overall cost of security.

Potential savings of up to $479 per device (£425 in the UK) across thousands of devices equate to millions in annual savings available to the conscientious mobility manager.

This paper therefore outlines not only how to calculate the true TCO of enterprise devices, but also how to manage the costs of each individual controllable line item, therefore reducing the TCO.

## Introduction

Enterprise mobility is essential to business. Whether a standalone productivity-based initiative or a component of a major digital workplace transformation, providing mobile access to corporate data is almost obligatory for the modern business.

But while the decision to invest in mobility is simple, the management of its cost is not. Unlike much of a company's infrastructure spend, mobility costs can spiral quickly and unexpectedly. Remedying security breaches, roaming charges and employees' excessive data use are all ways in which mobility risks and costs can escalate suddenly.

This rapid and seemingly uncontrollable cost escalation is something that IT departments didn't need to worry about in the past. While IT infrastructure spend is often predictable and manageable. Mobility simply doesn't play by these rules.

Because of its ability to catch IT departments unaware, we chose to examine exactly which areas of spend make up the TCO of enterprise mobility. Questions that we endeavor to answer in this report include:

- What is the typical TCO in the US and the UK?
- Which element(s) of ownership entail the greatest cost?
- Of all the cost factors, which ones are controllable?
- How does company size and operating system affect the TCO?
- To what degree can security measures and practices reduce the TCO?

This is the world's first study on the total cost of ownership of enterprise mobility. Given our visibility of hundreds of thousands of enterprise devices across the globe for some of the world's largest and most security conscious companies, we are in a unique position to offer this insight.

We structured our TCO analysis into five different areas of cost:

- Hardware
- Carrier charges
- Services
- IT resource
- Security

Hardware and carrier charges are what most IT departments consider to be the entire TCO. Some, especially those who are deploying their own applications or are using an EMM platform, also include services. However, few think to include the IT resource, and especially not security.

We elected to pull security out as a specific area of the TCO, rather than incorporate it within IT resource or services. It represents a large and growing area of unknown and unpredictable spend, especially in these times of XcodeGhost, Stagefright and other widespread mobile malware infections.

In particular, we have recently seen high profile breaches at Sony, Target, Ebay and TalkTalk. Their true cost is hard to quantify. But as this report shows,  greater spend on prevention is the key to reducing the even greater spend on remedy.

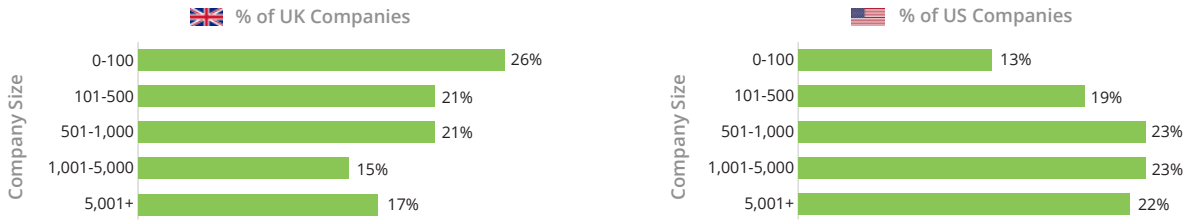
## Methodology and background to respondents

Wandera commissioned independent market research partner, Redshift Research, to support this study. Redshift Research collected responses from 1,000 IT respondents spread equally in the US and UK, all of whom had affirmed they had responsibility for either the selection, procurement, financing or management of mobile devices within their organizations.

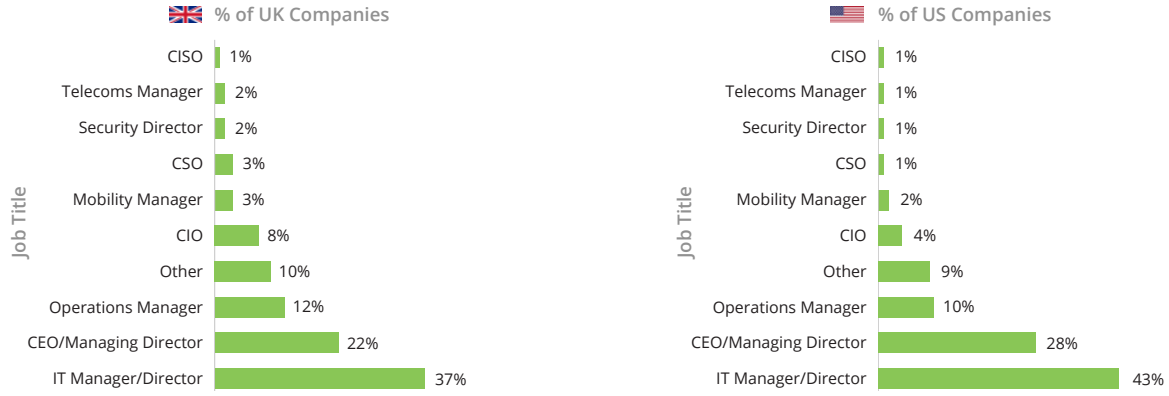
The statistics in this study are based on the average spend for one corporately liable device over one year. For hardware costs, respondents had affirmed they had invested in new devices within the last 12 months.

Where applicable, this study uses a currency conversion rate of $1.53/£.

**Breakdown of respondents' company size:**




**Breakdown of respondents' job titles:**




**Breakdown of mobile estates by OS:**
(using the OS that comprises more than 50% of the entire mobile estate)

## Core TCO Findings

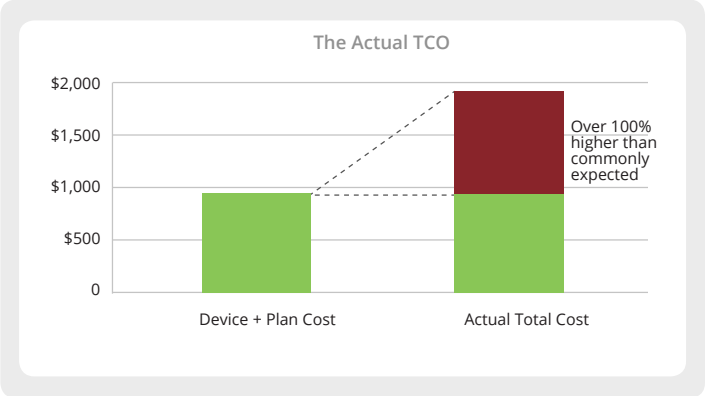
The typical CIO's approach to calculating the TCO of an enterprise device is to start with the device cost then add the cost of the data plan. On occasion, they may add the cost of a bill shock event (additional unexpected charges for exceeding carrier plans, or roaming charges etc.), but these will often be simply dismissed as frustrating overages and not considered in ongoing budget calculations and TCO conversations.

As a result, too many enterprises believe their TCO rarely reaches beyond $1,000 per annum. But we can see from this study that this significantly underestimates the true costs.

Mobility managers need to incorporate additional carrier costs (such as anticipated overages and roaming bundles) as well and additional hardware costs (such as accessories and peripherals) within their TCO calculations. But what about the the spend on Enterprise Mobility Management (EMM) platforms? Or the cost of IT management hours? Or security – both in terms of mobile security software, and the costs of remedy where mobile data was accessed illegally?

All these elements count towards the TCO. In which case, why are they so rarely included?

This report shows just how dangerously unrealistic the current perception of TCO is. Rather than the typically perceived $853 (or £628 in the UK), our research has discovered that the average TCO is in fact $1,840 (£1,272 in the UK). The actual TCO is 116% higher than commonly expected by most mobility managers in the US (103% in the UK).

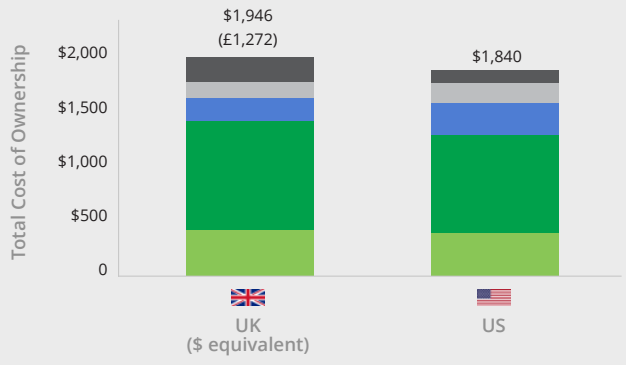



Too few enterprises are including important line items in their TCO calculations, and so are considering their mobile estates to be cheaper to run than they really are. If this erroneous belief persists, then readily-available and easily-implemented cost-saving measures will be missed. And all while mobile running costs continue to accumulate.

**Average TCO by territory:**

Overall, TCO is on average 5% less in the US than in the UK. This is of course not a massive discrepancy – and perhaps even one that can be explained away by being within the margin for error. However when the individual areas of spend are assessed, and particularly when they are broken down by company size, interesting differences appear.

For instance, hardware spend is 6% higher in the UK than in the US. And what is it about managing corporate mobile devices in the US that means that spend on services and IT resources is so much higher than in the UK?




| | UK | US |
|---|---|---|
| Security | £136/11% | $113/6% |
| Services | £102/8% | $181/10% |
| IT | £129/10% | $273/15% |
| Carrier Cost | £639/50% | $888/48% |
| Hardware* | £266/21% | $385/21% |
| **Total** | **£1,272** | **$1,840** |

*Where devices are refreshed every 2 years costs have been annualized. Where carrier contracts include free devices these costs have been seperated out.*

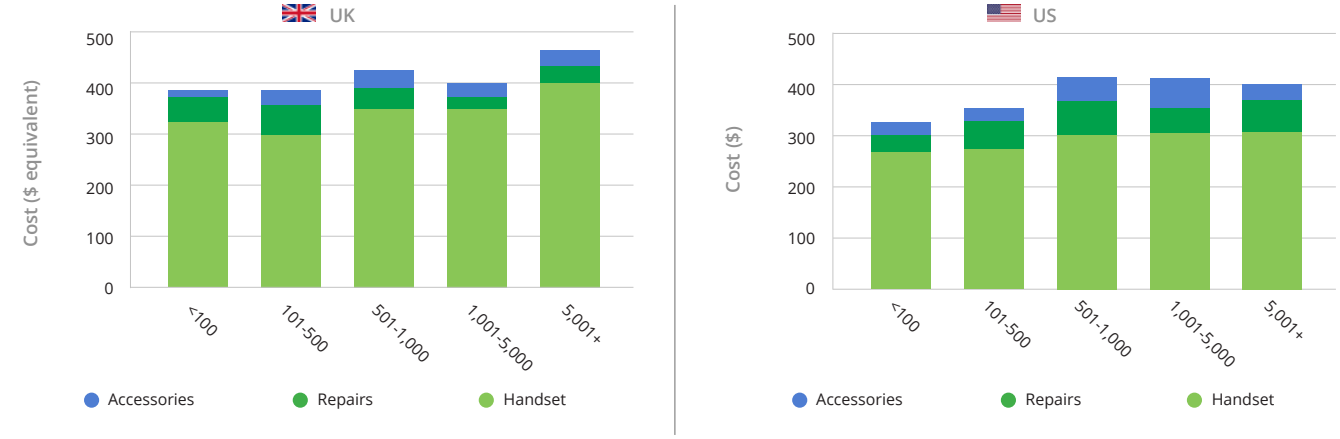
## Hardware

Unsurprisingly, handsets make up by far the greatest proportion of the hardware cost. But UK companies pay as much as 28% more than the US for their devices, simply because of higher device costs in a less competitive market.

The largest companies pay the most for individual handsets as they tend to be more focused on functionality and specification (greater memory, larger screens etc.) than saving cost. To put this into sharp focus, the UK's largest companies for example spend 23% more than the average spend by smaller companies.

Meanwhile, small to medium-sized companies in both countries (101-500 employees in the UK; 501-1000 in the US) pay the most for repairs. Larger companies are offered better in-built support by carriers for repairs and exchanges, and they have the ability to afford extended warranties and better insurance policies.

Sometimes carrier contracts may include a device for free but the cost of this device is actually a large part of the monthly charges. Where this is the case, we have seperated out the device cost from the true carrier cost. Furthermore, devices are usually refreshed every two years, and therefore replacement costs have been annualized.

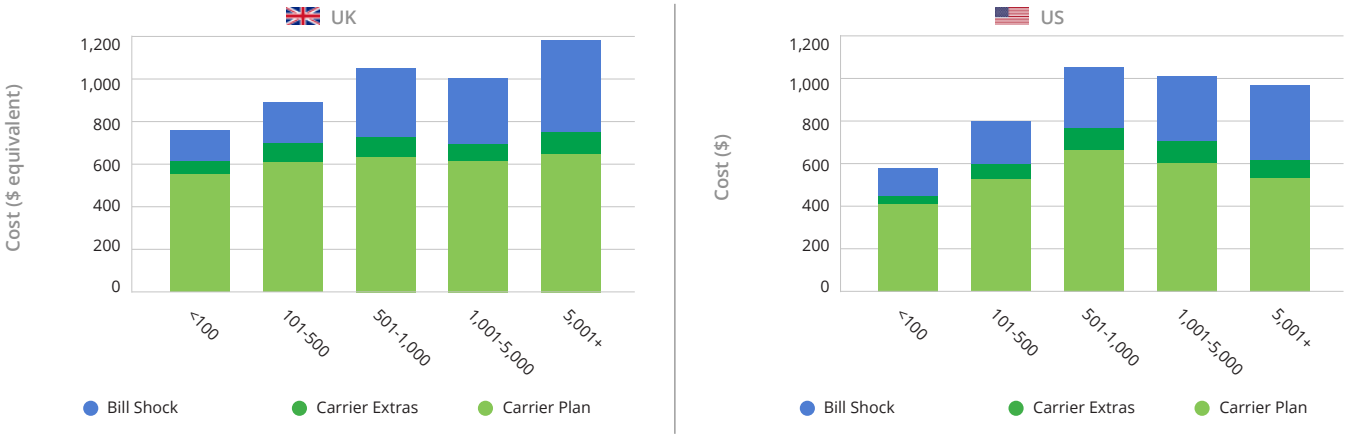



*Small to medium companies are incurring the highest costs for each handset repair*

## Carrier Cost

In the UK, carrier plan spend is largely flat, irrespective of size of company. In the US, there is a clear rise and fall in carrier plan spend as company size increases. The economies of scale clearly take effect once a company reaches 1,000 employees or more.

It is mainly 'bill shock' that causes the greatest fluctuations, showing clearly that bill shock education is sadly lacking in the largest companies, with a far higher proportion of 'roaming' employees versus 'domestic'. So why is bill shock so dangerous for enterprises? It's the second greatest single contributor to overall TCO for 5,000+ enterprises, as opposed to only the fourth greatest for most other company sizes. But why?

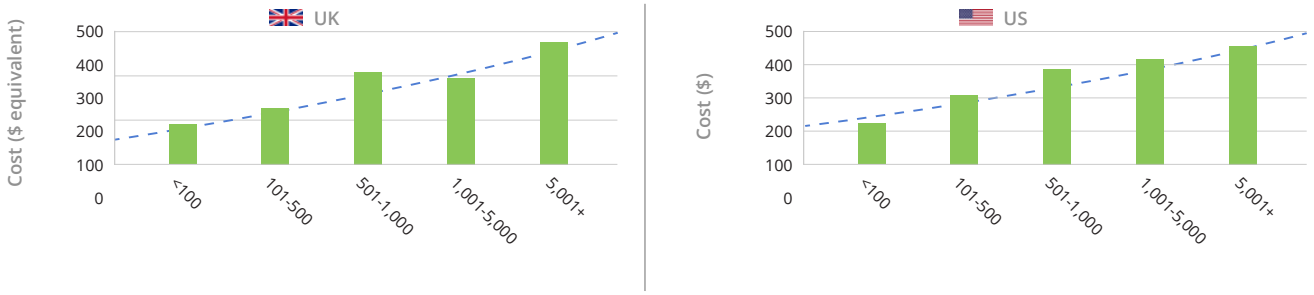



*The largest US companies are paying less for carrier plans than the largest UK companies in addition the largest US companies are paying less for plan extra packages*

## Bill Shock in detail

Larger enterprises are, generally speaking, less cost sensitive than smaller ones – this is illustrated by the typical spend on devices. Larger enterprises therefore tend to employ less scrutiny over an individual employee's excessive data use or roaming charges, and they are more likely to require their employees to travel to emerging countries where data costs can be extraordinarily high.

But this lack of cost sensitivity leads to trouble, especially in the US. Carrier costs as a whole – including the core plan and extras – are higher in the UK, but bill shock costs are overall dramatically higher in the US. This is through a combination of factors. Firstly, US charges for going 'over plan' are more punitive than in the UK. Secondly, the UK benefits from EU-based roaming agreements, whereas the US does not have similar agreements.



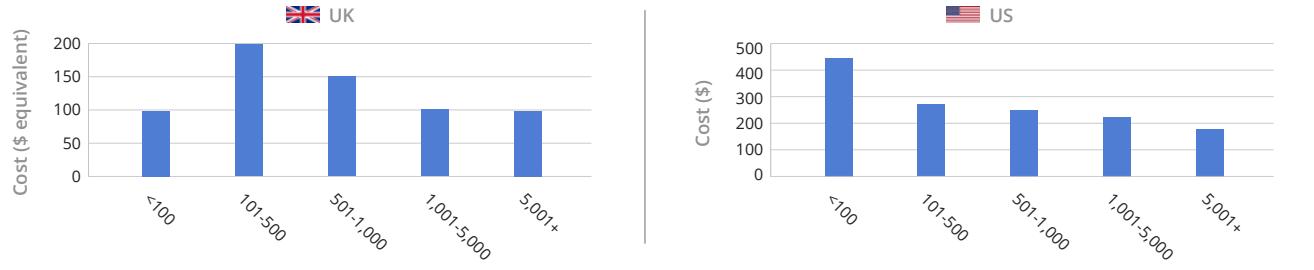

*Bill shock events generally increase with company size as a larger proportion of the workforce is roaming*

## IT

Interestingly the US spends a great deal more on IT resource per device than the UK. However this is largely explained by generally higher IT employment costs. Small US companies pay the most per device for IT/staff resources.

With the exception of the smallest UK companies, the smaller the company, the greater the IT resource overhead per device. Larger companies are naturally able to spread their IT resource investment across more devices, bringing the individual device TCO down. Costs are further reduced through greater use of outsourcing of IT management which is usually only available to larger companies.

As will be shown in the next section, this size-based difference is also caused by larger companies being more likely to use additional tools and platforms that assist in the proactive management of devices. This is clearly an investment that is not made by most smaller companies, but that does reduce the burden on the IT function for the enterprise.

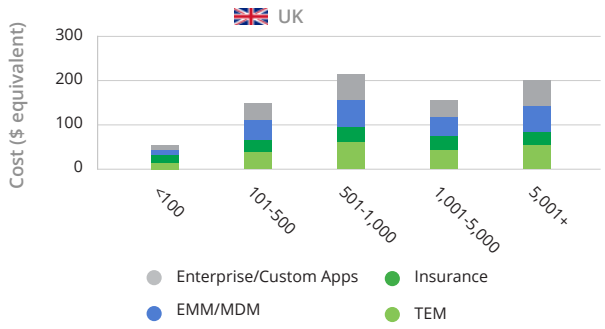


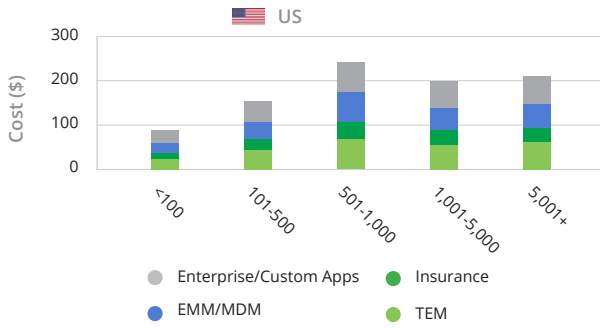

*Smaller US companies are paying the most per device for IT/Staff resources*

## Services

As touched on above, it is understandable that smaller companies spend far less on services such as telecom expense management (TEM), insurance, enterprise app stores or enterprise mobility management (EMM). They would rarely have the number of devices or the need to justify the investment, hence spend increases with company size.

However, there is a noticeable and surprising difference between the degree of spend in the US and in the UK. The US appears to be more willing to pay more for higher specification services and be an earlier adopter of such technology than the UK.




*Smallest companies have a lower take up of services*

## Security

The most surprising revelation from this data is the cost of remedying a security breach. It is on average three times the amount being spent on security software.

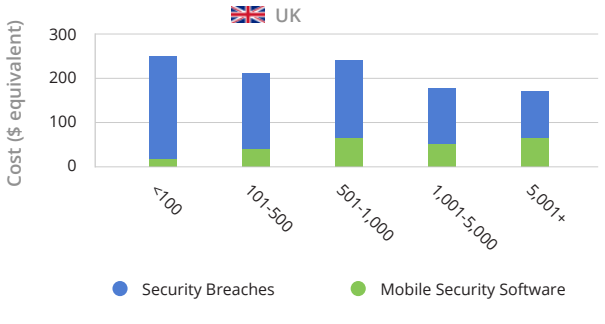
The security breach spend of larger companies is less than that of smaller companies, despite larger companies spending far more on mobile security software. This is because the cost of a breach far outweighs the cost of suitable protection. The lesson is therefore clear: invest comparatively little now and sidestep future massive clean up costs in the future.

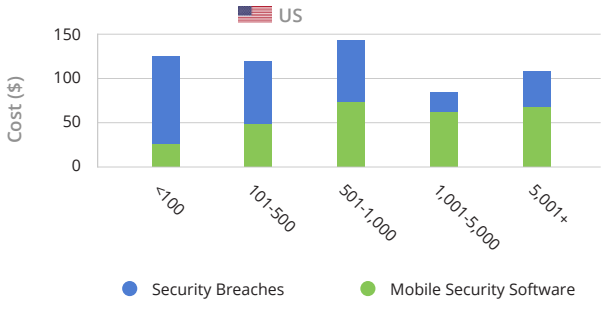
The case for improved mobile security was highlighted by 23% of our global respondents reporting having suffered a mobile security breach in the last 12 months.

In the UK, where 18% of respondents had suffered a mobile security breach, the greatest proportion of these companies (20%) said these breaches had cost their companies a staggering £25,000 to £100,000 – with an only slightly smaller proportion (19%) lamenting spending between £100,000 and £250,000.

Meanwhile in the US, 28% reported a mobile security breach in the last 12 months. A quarter of these companies admitted that the breaches had cost their companies between $40,000 and $150,000. Only a fraction fewer respondents – 23% - said the breaches had cost them between $150,000 and $400,000.

These are clearly far greater losses than any mobile security investment.

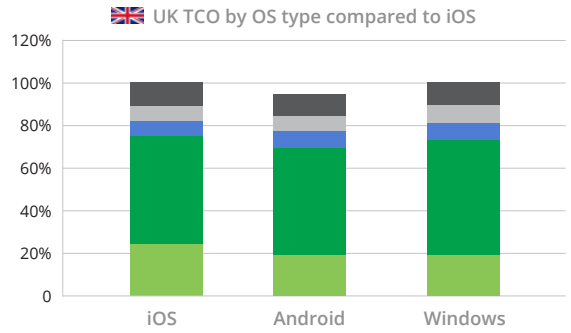


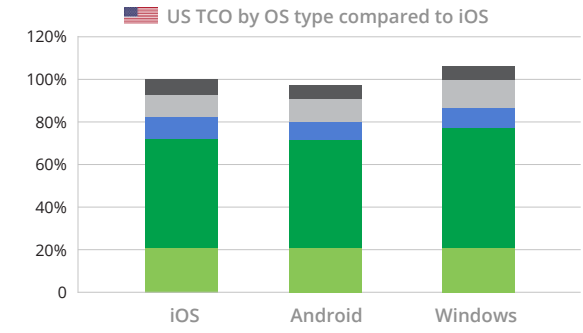

*The security spend for larger companies is a third less per device than for smaller ones*

## How OS impacts TCO

In both the US and UK, mobile devices with Android OS deliver the lowest TCO, and Windows deliver the highest (joint highest in UK). This is despite Apple being the most expensive device type.




| | iOS | Android | Windows |
|---|---|---|---|
| Security | 11.0% | 9.9% | 9.5% |
| Services | 7.2% | 8.1% | 10.1% |
| IT | 7.2% | 7.2% | 7.7% |
| Carrier Cost | 50.3% | 50.2% | 52.6% |
| Hardware | 24.3% | 18.9% | 19.1% |
| **Total TCO** | **100%** | **94%** | **99%** |
| Difference to iOS | - | -6% | -1% |




| | iOS | Android | Windows |
|---|---|---|---|
| Security | 5.9% | 5.7% | 6.6% |
| Services | 11.4% | 11.2% | 14.5% |
| IT | 10.8% | 9.7% | 10.9% |
| Carrier Cost | 52.4% | 50.7% | 58.3% |
| Hardware | 19.5% | 19.7% | 21.9% |
| **Total TCO** | **100%** | **97%** | **112%** |
| Difference to iOS | - | -3% | +12% |

## Controllable vs Inevitable Costs

So far, we have discovered that:

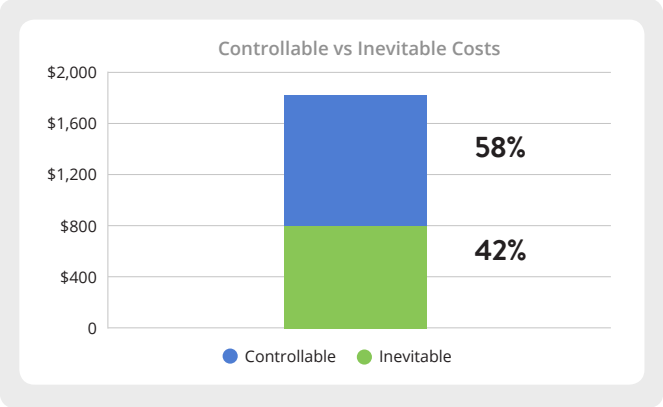
- Overall costs in the "hardware" category are led – unsurprisingly – by the cost of the device
- The US suffers from the most punitive charges for exceeding pre-set carrier plans, and yet enterprises struggle to prevent employees from going beyond their limits.
- IT resource burden per device is less in larger companies, mainly because they are able to invest in proactive management platforms and other services that reduce reliance on IT teams.
- The age-old security industry claim of prevention being cheaper than remedy is proven once again, with enterprises benefiting from being able to spend more on security software and therefore reducing the number and cost of illegal data breaches.

But against the backdrop of these concerns, how can enterprises control their levels of TCO without impacting productivity?

Looking at the categories of spend, Hardware, IT and Services costs are largely inevitable - these are simply prices and fees that are dictated by third party manufacturers and market rates. However, carrier costs and security breaches are very much controllable and can be selected and adjusted to meet the budgetary needs of the company.

Data compression technology can minimize data requirements. Prudent usage policies including capping and blocking can ensure that access to unrequired content is restricted – even to the extent of removing as much as 30% of overall data used. And as we have seen, investment in security means a dramatic reduction in breach remedy costs.

This means that the proportion of controllable versus inevitable costs presents a very positive picture for SMEs and enterprises alike.

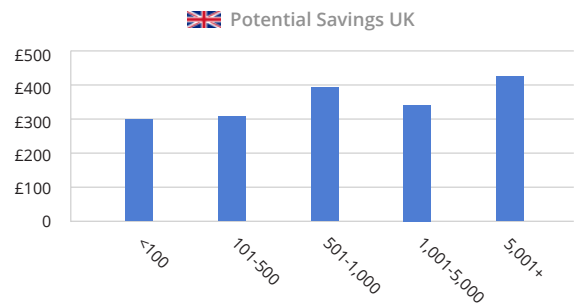


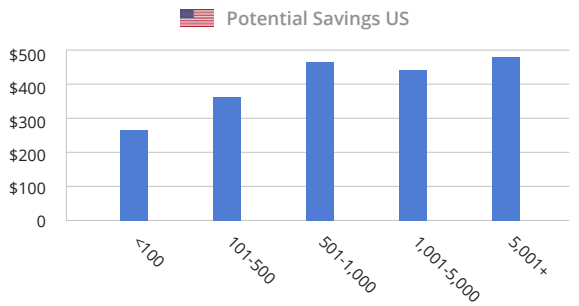

**58% or $1,090 (£710) of the TCO is able to be controlled and therefore reduced.**

It is important to note that these controllable costs should not be mistaken for removable costs. Based on our experience, data cost management is a process whereby many different levers can be manipulated to effectively manage mobile data costs. These include policies for domestic usage and roaming; bill shock prevention through usage caps and thresholds; and data compression to reduce the overall load.

We believe that a successful data cost management policy will introduce noticeable reduction into all the elements comprising carrier costs. For example, carrier plans can be reduced by 10%, carrier extras by 50% and bill shock can be removed completely.

Applying these typical percentage reductions to the TCO findings from this research, the gives the following available savings:



## Key Security Recommendations

As organizations adapt to mobile computing and it becomes part of the fabric of their services and the way they do business, we would like to provide the following recommendations to improve the effectiveness and security of your mobile initiatives.

Mobility can help transform your organization – your staff will use mobile devices in their work in some way so you are better off trying to control it and set the parameters and policy upfront – you need to stay ahead of the mobility risks to your company.

Specifically we believe that mobile security can be made more effective through these five recommendations:

1. User Education is key. If users unwittingly help hackers through, for example social engineering techniques and phishing, there is little that the OS provider can do to protect the device and the data.

2. Ensure that unnecessary financial information is not kept on users devices.

3. Security patching and updating of the OS is crucial for fixing vulnerabilities on a timely basis.

4. Ensure users only use legitimate and well-known app stores, are careful not to download clones of popular apps and read all the relevant app permissions as applicable.

5. Multi-level mobile security. We believe mobile security requires unrivalled access to real world data in real time to stop threats as you see them. Security needs to be multi-level: on the device, in the path of the data, and integrated to the device management software. This allows you to have a defense in depth approach which greatly improves your chances of early identification and remediation of the mobile threat.

## Conclusion

Enterprises' typical perception of TCO does not consider all factors that constitute the actual TCO. By not including security, services and IT costs within TCO – which are all legitimate additions and important considerations – enterprises face a huge additional 116% of unexpected costs in the US (103% in the UK).

A perfect storm is approaching where pooled data plans increase in popularity, but further reduce visibility into individual users' costs. Meanwhile, data usage levels will continue to grow exponentially due to increased tethering, music downloads, and over the top video streaming services such as Netflix. Many industry insiders are in fact anticipating that data usage of 14 GB per device per month will not be unusual by the end of 2017.

This means that with more opportunity and reason to use data and less visibility into individual usage, a real financial risk is coming to businesses who are not sufficiently rigorous in their mobile spend control. Usage visibility, end user education and administrative control are the best ways to stop mobility budget from leaking away.

In conclusion, a truly holistic approach is required to assess the actual total cost of ownership of an employee mobile device. In today's evolving mobile landscape, with significant financial and legal risks, enterprises must regain control of their mobile data, ensure full compliance, and prevent mobile security threats. The first step is to gain complete insights and visibility into the true financial costs they face from enterprise mobility.