adaptivemobile

adaptivemobile™
trusted network protection

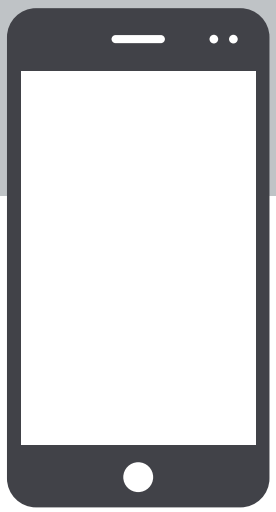
The Mobile Security Landscape in 2014

Securing BYOD in today's connected workplace

A report by:

harris INTERACTIVE®

The Role for Mobile Operators in Enterprise Mobility Security



Working with nine of the top ten operator groups and over 60 operators globally, protecting all services on fixed and mobile networks, AdaptiveMobile has unique insight into the global operator landscape.

Having seen mobile operators' services being commoditized by over-the-top cloud-based mobile device and security solutions, and the resultant erosion of mindshare and revenue from their enterprise accounts, AdaptiveMobile commissioned Harris Interactive to investigate the opportunity for operators in enterprise mobile security.

An increasing number of employees use their own mobile device for work.

The research showed that enterprises still provide employees with devices, but increasing numbers of employees use their own phone or tablet for work purposes:

- 93% supply mobile phones, 65% tablets
- Employees are relatively more likely to use their own devices than enterprise provided devices for work purposes
- 79% US, 77% EU enterprises allow employees to use their own devices
- And the proportion doing so could well grow as only 38% of employees are taking up the option to use their own devices right now

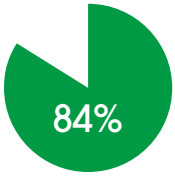
Enterprises have pursued this BYOD strategy, allowing remote access to their internal network and servers, believing they are adequately protected.

Over two-thirds of employees in both regions can access their company's corporate network.

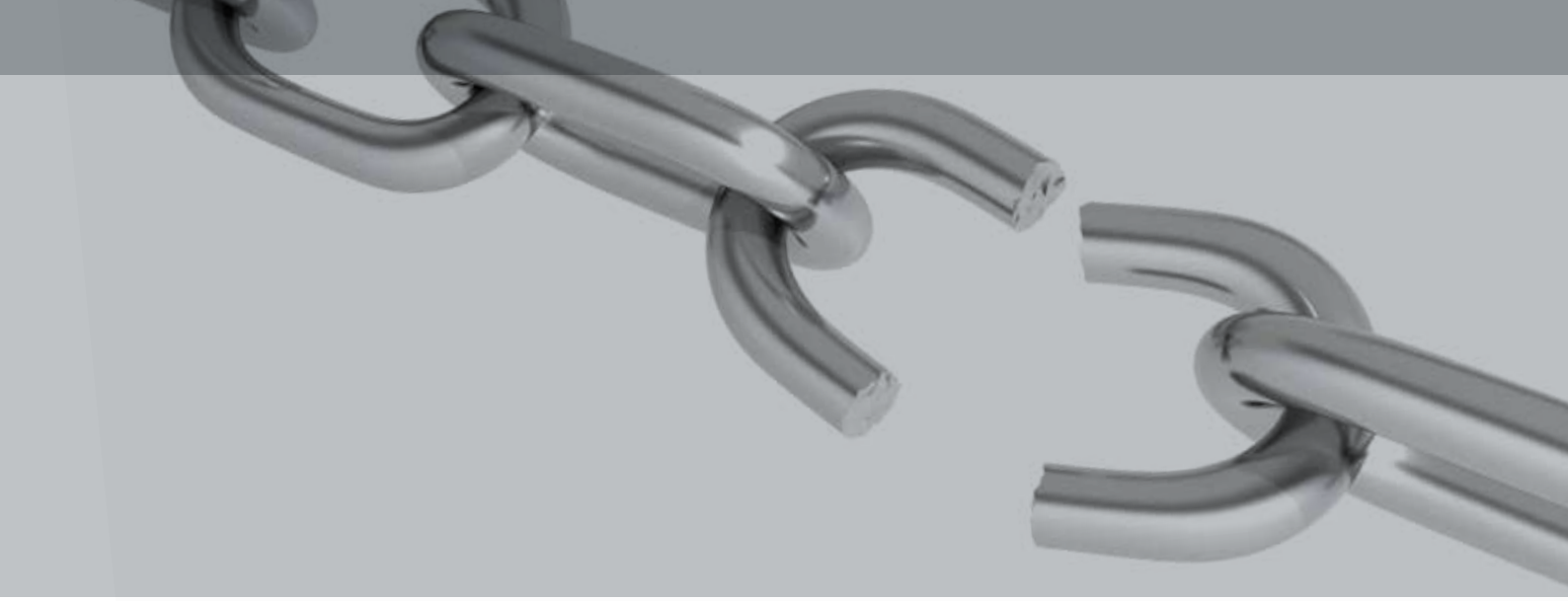
91% of businesses told us that they have controls and policies in place for dealing with mobile security breaches and the vast majority (93%) also agreed that they can detect and respond to mobile security breaches when they occur.

84% went further and claimed they are future-proofed.

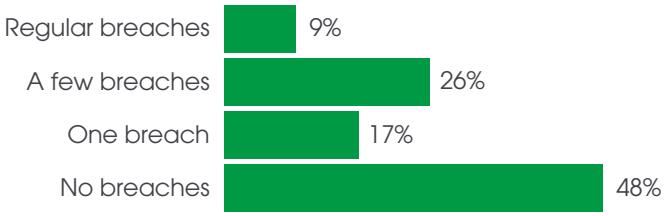
Claim they can detect and respond to mobile security breaches when they occur.



Believe their current mobile security solutions are future proofed.



However, 52% enterprises have experienced security breaches in the last year, and 35% on more than one occasion.



Two-thirds of enterprises do not have visibility of their top security threats.

Businesses typically use 4 or 5 mobile security solutions and almost two-fifths (38%) are sourcing these from multiple vendors. US businesses use more security solutions than those in EU and are more likely to source from multiple vendors.

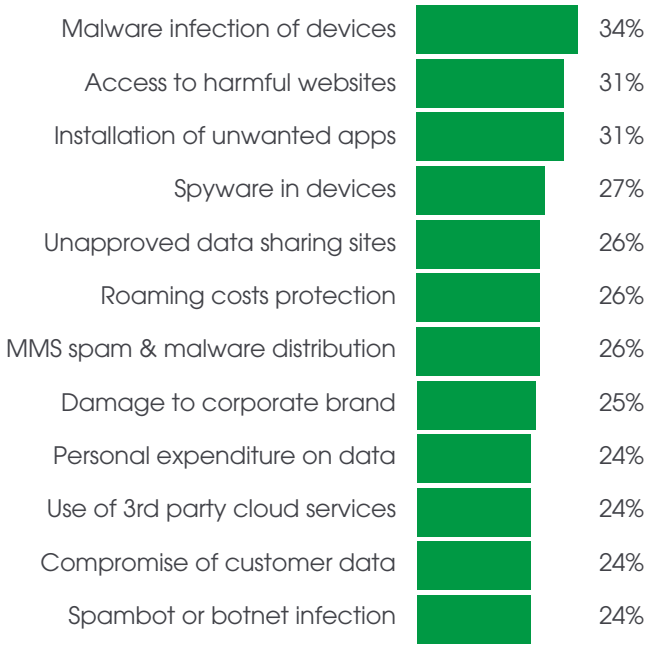
Almost two-fifths of businesses admit they have no visibility of what their employees are doing when they are using their own devices for work purposes and only one in three can identify common potential threats.

Hacking and lost company data are the main types of mobile security breach.

Many of these security breaches have very serious implications for businesses:

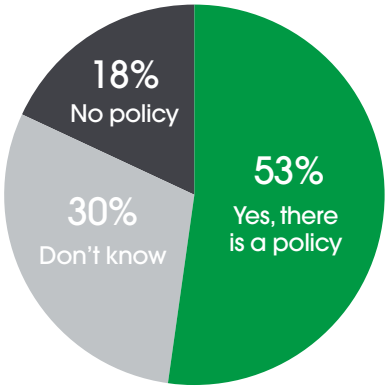
> "A minor security breach caused the company to lose about 10 percent of its running capacity."

> "We have leaked a lot of information to our competitors - mainly our strategy, our financial health and our weaknesses."



Employee ignorance of BYOD policies leaves enterprises open to increased levels of security breaches.

Only just over half (53%) of employees are aware that their employer has a specific policy in place for employees who use their own mobile devices for work purposes.
Three out of ten employees believe there is no policy in place at all and almost a fifth are not sure.



Only a minority of employees who use their own devices to access their company network are worried in any way about compromising their employer's business information security.

Only a minority of employees who use their own devices to access their company network are worried in any way about compromising their employer's business information security.

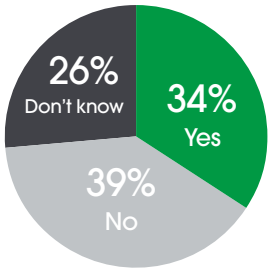
This lack of understanding on the part of employees may well be a factor in the high level of security breaches experienced by businesses and points to the need for a comprehensive solution that is readily understood by enterprises and employees alike.

Enterprises believe that employees know that there is a "cost of convenience" in BYOD.

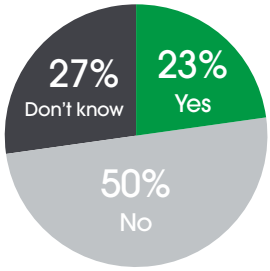
Of business that have visibility of employees' own devices at all times believe that employees are aware of this.

The reality is somewhat different however:

The vast majority of employees do not believe that (or are unsure whether) their employer can see what they are doing on their personal devices.



And just 23% believe their employer can lock or wipe their personal devices at any time.



And finally, a fifth (21%) of employees admit that they have no idea what control their employer has.

Employees would react negatively if they knew what level of visibility and control their employer has over their own devices when used for company purposes.

Data protection and privacy of personal activity are key concerns for employees, coming top of a list of criteria that are important when deciding whether to use a personal device in a work capacity. And when we tested what employees would do if they were to discover what employers can actually do...

Half said they would stop using the device if their employer had visibility at any time

Two-thirds would stop if their employer could lock of wipe their personal devices at any time

Those prepared to carry on using their own devices knowing the above, would typically be unhappy about the situation.

There is a clear implication here for enterprises – the significant cost savings and productivity gains they are making through BYOD would likely reduce significantly if employees were to discover how much control of their devices they have ceded to their employer. Given that current solutions in place are neither protecting the enterprise adequately, nor giving employees the personal protection and privacy they are looking for: is there an opportunity for operators to step in?

We tested reactions to AdaptiveMobile's Mobile Security Management (MSM) solution.

Enterprises

The AdaptiveMobile MSM service is a fully cloud-based platform providing companies with a full security offering to manage both employer-provided and employee-owned mobile phones and tablets.

Employees

The AdaptiveMobile MSM service is a cloud-based service that helps balance the requirements of an employer for security with the privacy and protection of an employee when using their own device inside and outside the office.

Key Features

- Web Policy Controls
- Roaming Policy Controls
- Device to Cloud Traffic Encryption
- Compromised Device Detection
- Application Policy Controls
- Device Controls
- Reporting and Management

The response to MSM was overwhelmingly positive from enterprises.

87% expressed an interest in discussing it with their mobile operator if it were available. There were also high levels of agreement with more diagnostic questions that were posed:

Levels of interest were high in both regions and particularly so in the US.

Comprehensive device security is the general message that resonates most with enterprises.

"It secures many aspects of mobile devices and addresses many different concerns."

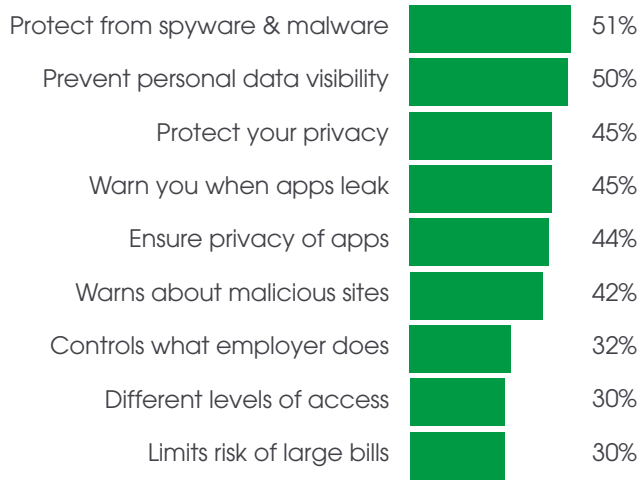
Employees also responded very positively to the MSM service description.

Two-thirds were interested in having MSM at their company if it were available.

And as with employers, the majority agreed that the solution is relevant, new and different and offers clear benefits over other solutions available.

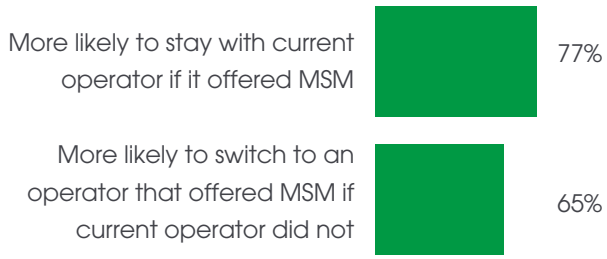
Additionally, 72% agreed that it provides the protection they need to use personal devices in a work capacity.

Data privacy is a key theme of the most resonant aspects of MSM for employees



There is an opportunity for operators to step in with an Enterprise MSM solution.

72% of business decision-makers would be likely to take the solution from their operator and MSM has the potential to act as a key retention and acquisition tool for operators:



Employees are also very receptive to the idea of taking MSM from their mobile operator.

The majority (75%) of employees feel confident that their mobile phone operator would be able to protect employers and employees alike if they were to offer MSM.

And a clear majority of employees (65%) would trust MSM more if it were offered by their operator, than if it was run by their employer.

In Summary

We discovered that:

- Enterprises believe they are adequately protected from mobile security threats, including being future-proofed.
- However, security breaches are still taking place, repeatedly in a third of businesses, and typically result in significant inconvenience and / or loss of earnings.
- Only a minority of companies have visibility of security threats despite having multiple solutions (often from multiple vendors).
- Employee ignorance of 'work from home' policies is leaving businesses open to potential breaches.
- And most employees are in the dark about the level of control their employer has over their BYOD devices and would stop using them if they found out – a financially damaging outcome for enterprises.

Responses to AdaptiveMobile's MSM service were overwhelmingly positive:

- 87% of enterprises were interested in discussing it with their operator if it were available and the majority found it relevant to their needs, new and different and offering clear benefits over other solutions.
- This is an outstanding response, particularly given that most businesses had previously expressed that they were confident in their current security solutions.
- Two-thirds of employees were interested in having MSM at their company if it were available.
- 72% business would take it from their operator and the vast majority said it would increase their loyalty to their operator and even encourage them to switch operators to get the service.

There is clearly a role for operators to play in enterprise mobile security and AdaptiveMobile's MSM service is an opportunity to fulfil this role.

Research Scope

AdaptiveMobile commissioned Harris Interactive, an independent market research consultancy, to survey to a robust and representative sample of business decision-makers and employees in the US and in three major EU countries.




In total, 1,007 interviews were conducted with business decision-makers and 1,005 with employees working in equivalent (although not the same) organisations.

All interviews were conducted online between 7th and 31st January 2014.

Decision-makers were screened to ensure that they have significant involvement in IT operations and strategy within their organisation.

All employees interviewed had to use a mobile device (mobile phone or tablet) for work purposes and this could be either a device provided by their employer or one of their own devices that they had agreed to use for work purposes.

The research focused on organisations with 250 or more full-time employees. Quotas were set to ensure a mix of 'smaller' (250-499) and 'larger' (500+) companies were included.

All business sectors were included in the research and the pattern of business types was broadly consistent across decisionmakers and employees surveyed.

About AdaptiveMobile

AdaptiveMobile is the world leader in mobile security, protecting over one billion consumer and enterprise subscribers worldwide, and the only mobile security company offering products designed to protect all the services on fixed, wi-fi and mobile networks. AdaptiveMobile's award-winning security products provide customers with real-time visibility into what is happening across their networks and the actionable intelligence to respond to these threats. Scaling from the largest global service providers down to the individual user, AdaptiveMobile offers the most comprehensive mobile security products available on the market today; as well as sophisticated revenue-generating security services – empowering consumers and enterprises alike to take greater control of their own mobile security.

www.adaptivemobile.com