Employees tell the truth about your company's data

How to make mobile devices safe for work and play

ARUBA networks

Table of contents

Executive summary

Your company's data is at risk. But the threat isn't from cybercriminals or bored teenagers, instead it is your own employees who are often unwittingly putting your data at risk by failing to ensure their mobile devices are safe and secure. This report assesses where the IT industry is today, looking at the trends and patterns found in our recent multinational survey and moving the conversation forward to provide a solution to the problems raised by the research. By the end, we'll make sure you recognize the attitudes driving sometimes risky employee behavior when handling work information, and also help you understand how this behavior can be mitigated by the right technology.

Introduction – the habit of a lifetime

Think back a decade or two. What kind of computer did you use at work? Would you have brought your own desk-sized home computer in to work? The simple answer is no. The reason is size (and convenience). What began with the mainframe, moved to the desktop computer and then the laptop has moved to the next step: the shift to the tablet and the cellphone. It's predicted that half of us will be using personal devices for work by 2017, and with shipments in consumer mobile devices continuing to rise despite the recession, it's more than a passing fashion – it's a growing habit.

> "It's predicted that half of us will be using personal devices for work by 2017"

We all know that businesses are moving to a more mobile way of working, and there's a good chance you're reading this on a mobile device. In fact it might be your own personal device that you also use for work.

Employees at your company are statistically likely to be doing the same thing, and although you and your IT department are able to have some idea of how prevalent this trend is, you can't guarantee the security of work-related data on these devices.

Sure, you can enforce some security measures, like adding password enforcement policies to email accounts accessed via personal devices, using two factor authentication, or trying to convince the workforce to only connect via VPN. But there are limitations to what you can do.

What you can't do:

- Prevent users from losing their mobile devices (and losing company data).
- Prevent users from giving someone else access to their personal/work devices.
- Prevent users from storing or editing work data on a device that the company doesn't know about.
- Prevent users from logging on to unsecured wireless networks.

> "No company can completely control on which device its data appears"

Your organization wants control, security, and visibility. Your employees want privacy; a barrier between work and play.

BYOD (bring your own device) intensifies the need for endpoint security, but it also diminishes the traditional all-seeing powers IT departments have long held dear. Bluntly, no company can completely control which device its data appears on, nor can any company completely lockdown all of its endpoints. However, you can deploy simple and easy-to-install tools that satisfy user interests while simultaneously handing control back to your IT department. Everyone's a winner.

This time it's personal

Aruba Networks has recently completed two separate studies into employee BYOD habits. The first survey, carried out in March 2013 by independent research house Shape The Future asked 3,014 people from select European nations (France, Germany, Spain and the UK) and two countries from the Middle East (Saudi Arabia and the United Arab Emirates). All of the respondents used a personal smartphone for work purposes.

The second survey was conducted by Kelton in February 2013, and asked 551 American business people about their own personal mobile devices and how they use them for work. Both surveys were identical in terms of the questions asked.

Context is everything, so to set the scene it is worth highlighting how many companies do not provide any type of mobile device for work purposes. Forty-four percent of European companies, 40 percent in the Middle East and 52 percent in the US do not provide a mobile device for work. So employees are choosing to bring their own, and, as we will see from the results, this has major security implications.

No passcode

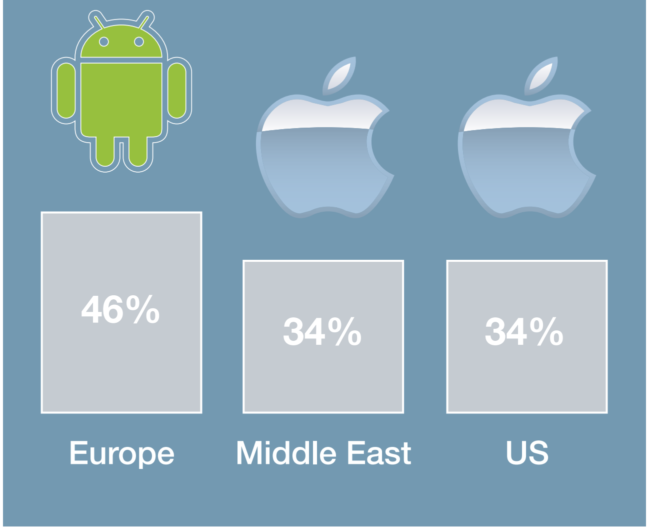
Nearly half (49 percent) of respondents in the US and an average of 43 percent across Europe and the Middle East do not have an automatic lock code or timeout function on mobile devices used for work. This means there's good news and bad news for corporate IT security: the good news is that more than half of workers recognize the hazards of working on mobile devices – they're easily lost or stolen – and have consequently and sensibly enabled passcode protection. The bad news is that a large chunk of users are leaving personal and work data wide open if their device were to fall into the wrong hands.

> "Fifteen percent in Europe have not told their employers that they use a personal device for work"

This is a problem squared when we look at the small but notable proportion of workers who have lost mobile devices: 21 percent in the US, 13 percent in the Middle East and 8 percent in Europe. Regionally, this response marks down US workers as being the most careless, followed by those in the UAE and then finally by Europeans. One-fifth to one-quarter (21 percent in Europe, 22 percent in the Middle East, 24 percent in the US) have provided phone access, including passwords, to another person. We're talking about personal devices, so this obviously isn't wrong, but it is food for thought for IT departments.

Employees are worried about their personal data, and that's making them less inclined to tell their IT department about their use of personal mobile devices. Fifteen percent in Europe and 17 percent in the Middle East and US have not told their employers that they use a personal device for work, 13 percent in Europe, 26 percent in the Middle East and 11 percent in the US would not report that their personal device had been compromised, even if it leaked company data. Additionally, at least two-thirds or more of workers across all regions would not report leaked data immediately, while 19 percent in Europe and the Middle East would never report the leak.

Apple to the core



This reticence is driven by perceptions of corporate IT departments. Namely, what the IT team might do to their precious personal device and data; users are understandably (but almost certainly unnecessarily) concerned about privacy. Twenty-five percent in Europe, 31 percent in the Middle East and 45 percent in the US worry about IT department access to their personal data. Perhaps more worryingly, 26 percent in the Middle East and 18 percent in Europe fear their IT department would interfere with their private data if they handed over their device.

When asked how they would feel if their personal data were accessed by their IT department, around half of all users across Europe and the Middle East described their reaction as 'angry', and 41 percent in Europe, 47 percent in the Middle East and 46 percent in the US would feel 'violated' by this news.

Regional accents

When asked how they would feel if their personal data was accessed by their IT department only 20 percent of US respondents reported they would react with anger, compared to the German (67 percent) and European average (52 percent), suggesting Europeans place more importance on privacy.

These responses clearly explain why users are holding back devices from the gaze of IT staff. Losing personal data is the number one concern for workers using personal devices, with US users being most worried at 66 percent. Europe is second at 45 percent and the Middle East at 40 percent.

You can't please everyone all the time

Employees clearly have concerns, and it is the nature of the unstoppable BYOD trend itself that employees feel they have to keep personal mobile devices away from their company IT department. This challenge is further illustrated by the 34 percent in Europe, 35 percent in the Middle East and 51 percent in the US that claim their IT department takes no steps to ensure the security of corporate files and applications on their personal devices. This will come as no surprise if the IT department hasn't been told about the device!

"Employees resent the power their employers now wield over their personal data"

The contradiction arrives when software is mentioned: 61 percent in Europe, 53 percent in the Middle East and 42 percent in the US say their IT department does not provide extra security software to protect work data on devices. A small but worrying percentage of employees think their employer's motives are suspicious: 18 percent in Europe, 24 percent in the Middle East and 31 percent in the US are concerned that adding security software will give their employers access to personal data.

"Dear client, I love you."

Nearly a third (31 percent) in Europe and 38 percent in the Middle East are worried about sending personal messages to professional contacts by mistake.

The research from both sides of the Atlantic shows how employees really think. It looks like employees and IT departments are gambling with data security, but chance isn't the only factor. In short, employees resent the power their employers now wield over their personal data, but are equally unconcerned about keeping company data safe. So, in order to maintain data security, is it time companies looked at new ways of separating work data from personal data?

Data from across the datelines

- Spain and the US are seemingly more concerned with privacy than other regions. On average, Spanish respondents want to keep 88 percent of their personal data totally private from the company IT department, compared to a European average of 56 percent. In the US, 36 percent want to keep all of their data private.
- The French are the best (or worst) at keeping personal devices from their bosses – 24 percent of respondents say their boss is not aware of their personal device and 57 percent say they would not declare a new personal device for work if they bought one tomorrow.
- Germans are the most cautious – only 17 percent have used their mobile device for private information.
- The English are relatively unconcerned about data violation: 21 percent would be 'indifferent' if their company took personal data.
- In Europe and the Middle East, women are more conscious of their personal data security than men. On average, women want to keep 88 percent of their data from their employees, compared to men (67 percent).

Conclusion

There is a clear disparity between what employees want and what IT departments need. Creating a division between personal data and work data would go a long way to solving these problems and putting employees' minds to rest.

To manage the use of personal mobile devices, it may be time to consider a separate, encrypted area on the devices for work applications and content. This gives IT full control over the corporate information in the encrypted space, but no visibility into personal areas of the device, thereby protecting employee privacy.

In the introduction we talked about the things you can't do regarding organization security and the rise of BYOD. But there's one thing you can do: investigate the changes taking place within your organization and understand the opportunities to make your workforce happy and your IT secure.

What the research means: Key takeaways

1. We are well past the 'BYOD is on the horizon' discussion, employers now need the tools to manage and maintain it, while employees are making BYOD real, right now.
2. Misconceptions about the role and remit of the IT department and the needs of corporate computer security are causing employees to keep their personal devices away from the IT department, for fear of compromising their personal data. This is jeopardizing company data.
3. Employers need to give their employees greater privacy for their personal data, but must also exert greater network controls to ensure that sensitive information is not leaked, without disrupting the user experience.

ARUBA® networks

www.arubanetworks.com

720 Centennial Court, Centennial Park, Elstree,
Hertfordshire, United Kingdom WD6 3SY
Tel: +44 (0)208 736 4574 | emeasales@arubanetworks.com