The Economist Intelligence Unit

A report from the Economist Intelligence Unit

The personalisation challenge

Business culture and mobile security

Big brother or big risk? The clash over privacy

Sponsored by

hp

Big brother or big risk? The clash over privacy

59% of employees who use their own devices at work are somewhat or very concerned that their employers have access to their personal information.

Privacy is becoming a flashpoint as more organisations allow employees to use their personal smartphones and tablets on the job. On one side are companies, which are rightly concerned about the security of sensitive and proprietary information on employees' personal devices. On the other are employees, who worry about employers snooping into their private lives by accessing personal information.

Tension is building. According to a January 2013 global survey conducted by The Economist Intelligence Unit and sponsored by HP, 59% of employees who use their own devices at work are somewhat or very concerned that their employers have access to their personal information. It is a valid worry, given the capabilities of today's sophisticated devices and the technologies and policies many companies impose in an effort to secure their data.

Smartphones and tablets contain very personal data, such as photos, videos, e-mails, text messages and histories of websites visited. They also contain social-network exchanges and records of users' physical locations and movements. Meanwhile, many organisations have put in place policies and implemented technologies that enable them to access this personal data as they endeavour to prevent security breaches and ensure reliable network operations. To some employees, their entire personal lives appear to be potentially on display to their employers.

As employees continue to mesh their personal and work lives on these devices, is there a safe middle ground?

Employer security vs employee privacy

Today, many companies simply take a hard line. Policies range from flat-out refusal to allow employee-owned devices in the workplace to reserving the right to remotely erase or 'wipe' all data on devices—including personal files—if the devices are lost or stolen or should the employee leave the company. "As an employee, you agree that if you are going to connect your device to our network and data, we reserve the right to wipe it," says Tony Young, chief information officer of Informatica, a US provider of corporate data integration software and services.

Programmes that allow employees to use their own devices for work "typically focus on employee benefits, but with benefits come responsibility," says Joe Nocera, a principal in IT security for PwC, a US consultancy. "Employees must agree to install security software, and, if something happens, they must agree to give up their devices."

Parting with devices causes the greatest anxiety among workers. "Employees are most worried about having to turn over their phone to their employer, who would then have access to personal content," says Stephen S. Wu, a partner in the US law firm Cook Kobrick & Wu LLP and author of the book *A Legal Guide to Enterprise Mobile Device Management: Managing Bring Your Own Device (BYOD)*.

While workers may view a remove-and-wipe policy as draconian, it is essential for the security of an organisation's systems. And, as one security expert notes, it can sometimes benefit the employee. “One organisation told me that the first time they had to wipe someone’s device, the company was really nervous,” says Rich Mogull, chief executive of Securosis, a US security research firm. “But the employee was actually thankful because he didn’t want his personal photos in hands of bad guys.”

Many companies also have policies that, in the event of litigation, require workers to turn in their personal devices so the company can capture a forensic image of the data—a policy that concerns many workers.

These policies also trouble many organisations, says Mr Nocera. “The device is owned by the employee, and therefore the concept of seizing it to perform an investigation is a little bit hard for organisations to embrace on day one.”

Mapping privacy concerns

Privacy concerns and expectations vary around the world. In our survey, anxiety about employer access to personal data is highest among Asia-Pacific respondents (72%) and lowest among European respondents (43%), with North America (62%) in the middle.

In Europe, privacy of personal data is often considered to be a fundamental right; the continent’s data privacy mandates are among the world’s strictest. Thus, Europeans may be less concerned about personal privacy because they are protected by stricter laws.

Mr Wu argues: “In the US, we are more worried about government surveillance, while Europeans are more worried about corporate surveillance.”

Views on privacy also diverge based on age. According to the EIU’s survey, younger workers are most concerned about employers having access to their personal information. In our survey, 78% of respondents aged 18-29 said they were concerned.

That may be because younger people have richer digital lives and so have more to lose. Or it may be a stronger sense of entitlement. “Younger workers, Millennials in particular, feel they should have unfettered access to whatever, whenever,” argues Phillipe Winthrop, founder of the Enterprise Mobility Forum, a US online forum that advocates best practices in mobility solutions.

Toward a more agreeable approach to policies

As more employees use their personal devices on the job, companies have found it increasingly necessary to implement meticulous security policies to protect business data, networks and applications.

These policies—remote wipe, in particular—may seem harsh, but organisations can take some steps to reassure worried workers.

“In training, the company could say: ‘We realize you may have personal photos and information on the device, and we will try to avoid accessing these files during discovery,’” Mr Wu says. “But they should know it may be almost impossible to avoid that.”

As for younger workers, who may have less experience separating their private and work lives, companies should clearly communicate the possible repercussions of using personal devices for business purposes, says Ed Stroz, co-president of Stroz Friedberg, a US investigations firm.

“You don’t want to scare your employees, but do you want to help them understand that, because something may occur that requires that IT look at the device, they should think carefully about how they use the device and what information they put out there,” Mr Stroz says. “They have to think about it in a different way than when they were in college.”

Another piece of advice? Always maintain professional decorum.

“The information I put on my mobile device is clean, and my posts to Twitter and Facebook are stuff that my mom would not disapprove of,” Mr Winthrop says. ■

> “You don’t want to scare your employees, but do you want to help them understand that, because something may occur that requires that IT look at the device, they should think carefully about how they use the device and what information they put out there.”
>
> Ed Stroz,
> co-president of Stroz Friedberg

Whilst every effort has been taken to verify the accuracy of this information, neither The Economist Intelligence Unit Ltd. nor the sponsor of this report can accept any responsibility or liability for reliance by any person on this white paper or any of the information, opinions or conclusions set out in the white paper.

London
20 Cabot Square
London
E14 4QW
United Kingdom
Tel: (44.20) 7576 8000
Fax: (44.20) 7576 8476
E-mail: london@eiu.com

New York
750 Third Avenue
5th Floor
New York, NY 10017
United States
Tel: (1.212) 554 0600
Fax: (1.212) 586 0248
E-mail: newyork@eiu.com

Hong Kong
6001, Central Plaza
18 Harbour Road
Wanchai
Hong Kong
Tel: (852) 2585 3888
Fax: (852) 2802 7638
E-mail: hongkong@eiu.com

Geneva
Boulevard des
Tranchées 16
1206 Geneva
Switzerland
Tel: (41) 22 566 2470
Fax: (41) 22 346 93 47
E-mail: geneva@eiu.com

Cover: Shutterstock