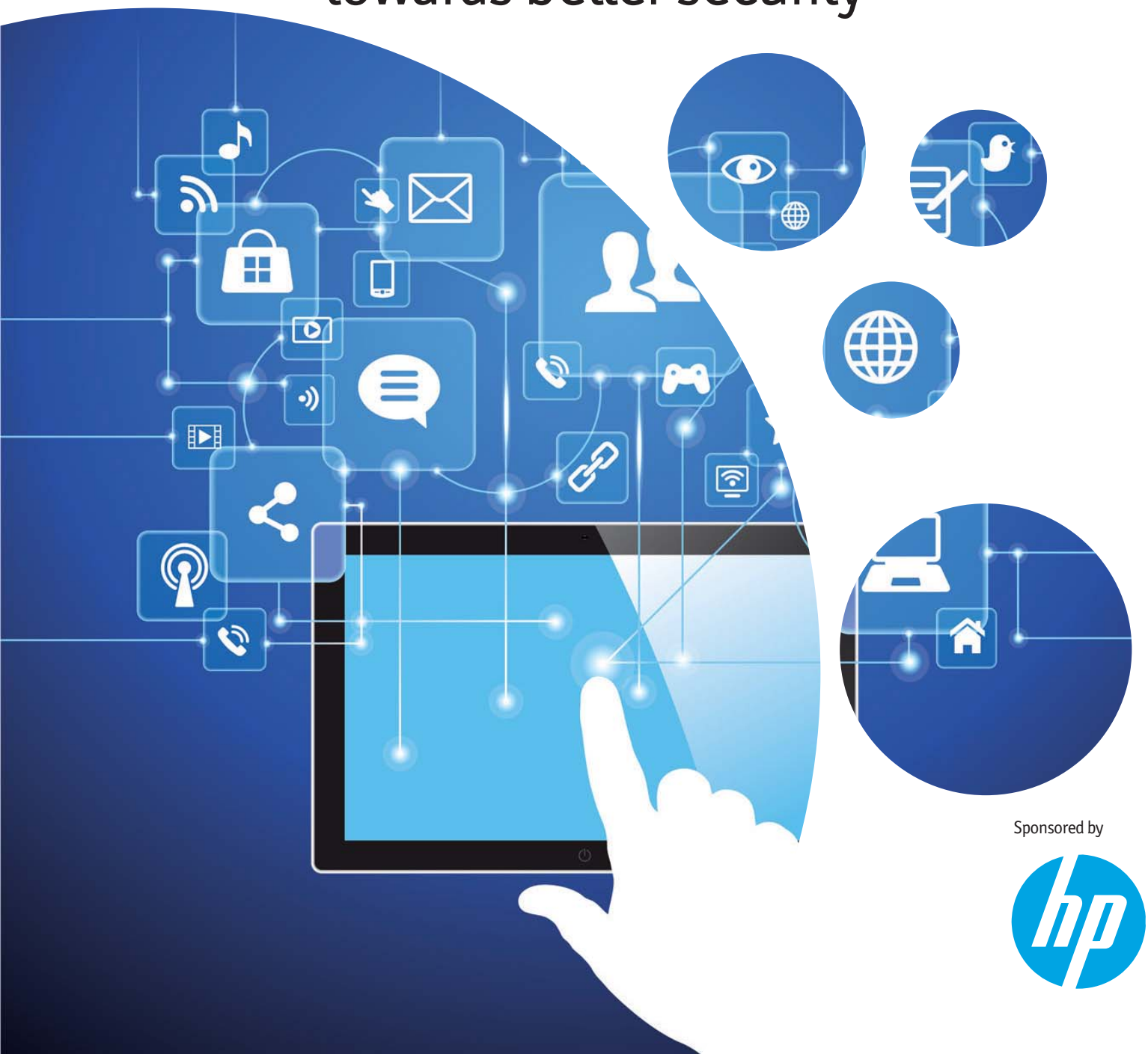
The Economist Intelligence Unit

The personalisation challenge

Business culture and mobile security

How mobile risks are pushing companies towards better security



Sponsored by

hp

How mobile risks are pushing companies towards better security

Two unstoppable trends—omnipresent mobile devices in the workplace and rapidly evolving cybersecurity threats—are testing the mettle of corporate security policies.

And traditional security approaches, often based on complying with regulations and legal requirements that mandate a basic set of security controls, are buckling under the pressure, according to experts. "Previously, the security approach was one-size-fits-all, with a focus on end-to-end security and compliance," says Joseph Nocera, a principal in IT security for PwC, a US consultancy. "What's needed is a risk-based approach, which is less about perimeter security and more about focusing on the security of your valuable data."

Yet many companies appear to be struggling to change course. A global survey of 316 executives in January 2013 by the Economist Intelligence Unit, sponsored by HP, shows that only 49% of respondents believe that their company's security policies are driven by the goal of risk reduction, while 58% believe that they aim to satisfy compliance and legal requirements.

Neglecting risk is dangerous when it comes to mobile devices, which present risks different from those of desktop computers. These devices can be easily misplaced or stolen, for instance, and no current security technologies can alert a company that a mobile device has been compromised, says Dan Guido, co-founder and chief executive of Trail of Bits, a US IT security firm. Moreover, in addition to valuable company data, they often hold a trove of personal data—especially devices owned by employees.

> "People are forced to think about data and about who has access to it and in what context. That's a positive thing, overall."
>
> Dan Guido
> co-founder and chief executive at Trail of Bits

These challenges have a silver lining, though: they push companies to reorient security around the data itself, a hallmark of new security thinking. "People are forced to think about data and about who has access to it and in what context," Mr Guido says. "That's a positive thing, overall."

Prioritising security based on the value of data

As reports of data breaches make headlines with alarming frequency, companies are beginning to realise that it is no longer feasible to block every attacker. The key, experts say, is to employ a risk-management approach that identifies, locates and safeguards the assets that really matter.

This is necessary, in part, because sophisticated intruders are aggressively targeting critical intellectual property, often a company's most valuable asset. Risk-based mobile security requires that companies first identify those assets, then classify their value and assign levels of importance based on that value estimate. Next, they must determine whether they will allow these data assets to be stored on mobile devices themselves or only on a server where they can be protected by layered network defences and access-control policies.

Some applications store data in mobile devices' working memory, which is vulnerable to malware attacks. Companies can mitigate this risk by limiting the data stored on devices and put in place polices that ensure mobile apps are in line with the company's security policies. In addition, companies can encrypt data on these devices.

When it comes to the devices themselves,

© The Economist Intelligence Unit Limited 2013

companies ought to determine which hardware will be permitted to access valuable data. "Just because you allow employees to use personal devices doesn't mean it's OK to use any kind of device with any kind of software with any kind of configuration," says Ed Stroz, co-president of Stroz Friedberg, a US investigations firm.

He recommends that companies create a tiered list of preferred devices and approved apps for those devices and then ensure that they meet strong encryption and authentication standards.

In general, Google's Android operating system is far more vulnerable to attack than Apple's iOS. The vast majority of malware targets Android, which, unlike iOS, allows installation of apps from an array of sources, rather than from a single, highly controlled app store. Moreover, distribution and application of security patches are slower and more complex for Android devices than for iOS devices. However, Mr Guido notes that devices sold by Google under the Nexus brand are supported by Google and receive software patches significantly faster than other Android models.

> "If you try to lock down the employees' environment, it's like putting them in jail"
>
> David Willis, chief of research for mobility at Gartner

Getting employees on board with the security programme

Companies should also put in place employee-related policies that can reduce corporate risk. For instance, they can secure the right to erase all data on devices containing company information if a device is lost or stolen or if the employee leaves the company. Such policies should specify that personal data stored on the device may also be deleted—and that the company will not be responsible for loss of that information.

It is also wise to get employees' confirmation in writing that they understand and will adhere to security policies, such as use of company security software and data encryption, requests to temporarily hand over their device for e-discovery and use of company-owned applications for valid business purposes only.

Crafting effective mobile-security policies requires input from an enterprise-wide team of stakeholders that may include IT, compliance, records management, finance, marketing, human resources and corporate communications, says Nancy Flynn, executive director of the ePolicy Institute, a US consulting firm that advises companies on workplace technology policies. A review by legal counsel, she adds, is paramount.

The mix of worker and corporate data on a single device is a potentially volatile combination with serious legal implications. No policy is more contentious than the capacity to remotely delete all data. This can be a particularly thorny issue for multinational companies because regulations about personal data and privacy vary around the world.

When drafting these policies, companies should factor in the rights and work habits of employees; they may even want to survey employees on how they use mobile devices.

Ultimately, companies must balance mobile device policies with ease of use. Policies that are too restrictive might deter the use of mobile devices or cause employees to skirt the rules. "If you try to lock down the employees' environment, it's like putting them in jail," says David Willis, chief of research for mobility at Gartner, a US research firm. "They will get really creative about getting out."

The weakest link in a mobile security program is often the employee, and the risk increases as they gain around-the-clock access to corporate data. Therefore, a comprehensive, ongoing employee awareness and training programme—preferably one that enables employees to absorb the information deeply, ask questions and affirm in writing that they will adhere to security policies—can significantly help mitigate risk.

Certainly, mobile security risks can be managed. When it comes to the threat of malware, mobile devices are safer than Windows desktops—for now at least. And risks to company data from lost or otherwise compromised devices can be managed using security technologies and network-side controls that can block infected devices from accessing the network, restrict remote access to sensitive data stored therein and wipe any data off the device itself. But managing the risks requires focusing on what really matters: the data. ■

© The Economist Intelligence Unit Limited 2013

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

© The Economist Intelligence Unit Limited 2013