

BUSINESS & CAREERS

Time to BYOD — bring your own device



HI-TECH

**LUIGI
BENETTON**

Not so long ago, law firms dictated what types of smartphones — typically BlackBerrys — their staff could use for work.

This has been giving way to the bring-your-own-device (BYOD) trend, which may spell the end of the BlackBerry's near-hegemony in the workplace.

Some people attribute BYOD to Apple Inc.'s iPhone. In fact, BlackBerrys entered many companies in the hands of executives who demanded that they be connected to corporate networks. Now it has plenty of company, and the crowd seems set to stick around.

Shaunna Mireau suggests law firms embrace the newcomers. "If somebody is personally more efficient out of the office with an iPhone or a BlackBerry, why would we limit them in any way to something that doesn't work as well for them?" says the Edmonton-based director of knowledge management and libraries for Field Law.

In spite of the uncertainty spawned by device heterogeneity, maybe it's time to stop fighting the wave and learn to surf it instead. Consider the following tips for making your firm BYOD-friendly.

Mobile device management

A variety of mobile device management (MDM) tools, reminiscent of the BlackBerry handset management system, allow IT staff to manage mobile devices of all kinds remotely. This would include: wiping lost devices, resetting passwords, encrypting devices,



IPANDASTUDIO / ISTOCKPHOTO.COM

scanning for malware, enforcing policies and password protection, and filtering Internet content.

Among the big names in MDM are RIM's BlackBerry Mobile Fusion, which can also handle Android and Apple devices. (Control over non-RIM devices is "expected in 2012" according to RIM's website.) Apple offers Configurator, a free device management app.

Keeping data within the firewall

Mireau says Field Law has always had policies about keeping client data within the firm from the days of paper files, and the same policies apply to electronic records.

"We've made it easy for people to connect to their tablets and home desktops," she says. "Most of the things people put on their mobile devices are not client files. They are things like the rules of court or statutes they use all the time."

Tools such as Citrix or GoToMyPC allow devices running various operating systems to

access client data using secure connections, playing the role of "dumb terminals." Once those connections are severed, no data remains on the device.

Information ownership policy

Traditionally, employers have held sway over how company-issued devices are used because it is their equipment. "They have pretty strong rights," says Stuart Rudner, a Markham, Ont.-based partner in Miller Thomson LLP's labour and employment group.

With BYOD, searching and monitoring rights aren't as clear-cut. Employees can object to searches and monitoring of devices that they own and for which they pay the bills.

Rudner says companies can still use policies to gain the control they would have had if they owned the devices.

Encryption, authentication, apps

Regardless of who the devices belong to, they must be encrypted to protect their contents from

prying eyes. "People lose their mobile devices on a daily basis," says Kevin Lo, managing director with Toronto-based Froese Forensic Partners Ltd. "I need to know that if a phone goes missing, whoever finds it can't easily get data from it."

Modern mobile devices let security-conscious owners set access codes that must be entered before people can use them.

"But how do you push the policy?" Lo asks.

It's a valid question since many people claim to suffer from password fatigue, so they may not want one more password to remember.

"Every device uses a different type of security scheme," Lo adds. "With all this device fragmentation, it's difficult to implement a policy."

The same concerns apply to the hundreds of thousands of mobile device applications that are out there.

"In the Android world, the market is much more fragmented, so the quality of apps may be questionable," Lo explains. "People download apps without understanding what they do."

Since seemingly legitimate Android apps can come packaged with malware, Lo suggests seeking methods (perhaps using mobile device management systems) that allow IT managers to monitor the apps installed on phones.

Managers could conceivably whitelist certain apps and blacklist others, keeping undesirable apps off the company network.

Cloud policies

Smartphone users often resort to cloud apps, such as Dropbox, or free email services such as Gmail, to transfer attachments to other devices with larger screens.

“

People lose their mobile devices on a daily basis.

I need to know that if a phone goes missing, whoever finds it can't easily get data from it.

Kevin Lo,
Froese Forensic Partners

"You need a policy that explains what the cloud is, how it works, what the risks are," Rudner says, adding that policies can expressly prohibit services that may put client confidentiality at risk.

Look for cost-saving opportunities

Now that some employees use their own devices, employers pay them monthly amounts to cover business use of their devices. They then cut provisioning and avoid billing in an effort to reduce overall expenses.

Firms may offload support to manufacturers or carriers, who can provide loaner devices while carrying out any necessary repairs. Employers may also oblige staff who buy into BYOD to ensure support for their devices.

Since employees who choose their own devices are more likely to understand how to use them, training costs may also decline.

Rudner advises considering not just potential benefits but potential problems. "Don't just look at cost savings but also look at consequences, especially for law firms where confidentiality is crucial," he says. ■

EBS

ASSOCIATE POSITION

The firm of Evans, Bragagnolo & Sullivan is seeking an associate lawyer with two or more years of experience, preferably in family law with some general practice knowledge. The candidate must be willing to relocate to Haileybury, Ontario. Applicants must demonstrate superior writing skills and keen attention to detail. We are seeking an individual with good interpersonal skills, who also has the ability to multi-task as well as the desire to learn about and assist with a busy general practice.

This community oriented firm offers progressive compensation with commensurate experience, benefits and minimal bureaucracy. If you are a self-starter looking for a pleasant small town lifestyle, this could be the right opportunity for you.

Please reply in confidence with a detailed resume and references by no later than **July 30, 2012**.

We thank all applicants but only those selected for an interview will be contacted.

Apply to ddorington@ebslawyers.com

Evans, Bragagnolo & Sullivan is a full service law firm with offices in Timmins and Haileybury.

www.ebslawyers.com

Kain & Ball

Kain & Ball is a boutique family law firm located in Mississauga. We pride ourselves on our expertise in family law, professionalism and strong team approach.

Due to our continued growth we are currently seeking the following:

- *Intermediate Family Law Associates* with 3 to 5 years of experience.
- *Senior Family Law Associates* with more than 5 years of experience.

Ideal candidates should have excellent written and oral communication skills, excellent drafting skills and have the ability to work in a fast-paced environment.

This is an exceptional opportunity to work with experienced family law counsel as well as to maintain independent carriage of files. Kain & Ball offers a unique balance between family and career. The successful candidates will work in a dynamic collegial environment with first-rate support staff and be offered a competitive compensation package.

If you are interested in exploring these opportunities, please forward your resume to:

Alexis.Johnson@kainfamilylaw.com

We thank all applicants for their interest; however only those selected for an interview will be contacted.