BYOD

By: Barb Feldman

Word count: 1000

As organizations recognize the benefits of increased employee flexibility, mobility and productivity when they allow and even encourage employees to use their own laptops, tablets, and smartphones for work, the popularity of BYOD (“bring your own device”) is growing. And because employees may be eager to buy the latest and most technologically sophisticated devices for their own use, BYOD policies can also result in savings for the company in terms of updated equipment and lower IT costs. But companies must have BYOD policies formulated and in place before they allow their employees to use their own devices for work.

Like many mortgage professionals, the brokers at Mortgage Architects are self-employed and responsible for buying and maintaining their own business equipment. Although the company recommends certain brands and set-ups, says Senior Vice President Alice Chan, brokers are free to choose the laptop or cellphone they prefer, although the company controls how brokers store and transmit data. Each broker uses his or her own login account to upload documents through the company’s secured internet portal, and to access a centralised library of business statements, reference material and marketing templates. Although the company has standard notification procedures for customers if brokers’ devices are lost or stolen, Chan adds, “provided our brokers follow our recommended best practices in protecting customer’s private information, there is no risk in using their own devices.” Agents must treat client

information diligently and adhere strictly to PIPEDA (the Personal Information Protection and Electronic Documents Act), adds Kathryn Kotris, the company's Vice President of Compliance. Because banks require personal information in the underwriting process, she notes "we have people's social insurance numbers, tax returns, salary letters, pay slips, bank accounts," she says. "We wouldn't leave anything in a briefcase in our car – that's how we must treat our mobile devices."

Harsh Pabla, CEO of Nanotek Consulting Corporation, is an enthusiastic promoter of BYOD when combined with cloud computing. Nanotek provides its clients with IT systems integration, infrastructure management and customized software. With cloud computing no information is stored on the device, he says, so whether the platform is accessed from an Android, iPhone or from a Windows desktop, as soon as his company has been notified of a compromised device it can be wiped remotely with Mobile Device Management (MDM) software. "You lose absolutely nothing other than the value of the device."

"If you're using Gmail or Hotmail, that's cloud computing," Pabla explains. "You're accessing your e-mail but you don't know where that server is or where that e-mail is stored. Cloud computing is basically a group of computers put together in a data centre outside your office." He says that there are huge advantages to cloud computing over older technologies, including no upfront costs. "You don't need to purchase any servers, any backup, any storage, you don't need in-house IT staff. You don't need to worry about upgrades, updates, patching, security – it's all taken care of for you." He explains that shared costs are lower "in the cloud" because infrastructure is being used to its maximum, whereas in typical segregated or local community environments only about

10 to 20 per cent of capacity is used. Information is also much more secure than it would be locally, Pabla adds. “In a cloud computing environment the information is stored in a triple-A military-grade data centres where people cannot walk in without proper access. There are security guards, cameras and other means of security.”

But whether an employee uses her own device to access work e-mails or type up notes on client meetings, that information might be stored on that person’s device, not solely on the company’s secure server, according to Adrian Miedema, a lawyer with Dentons who advises employers on strategic and risk management considerations in employment policy and contracts. For the employer the most important question must be “Can we control and protect the security of information that is on a device other than one the company owns?” he says. “That’s going to be a major consideration, particularly for employers that are in businesses where confidential information is a sensitive issue.”

There are also other issues as well. He points out that companies often have insurance coverage for data security issues, but such coverage may not automatically extend to employees’ personal devices. And since a client’s relationship is not with the individual employee but with the company, “it’s the company that is going to bear the brunt of a security breach,” even if the employee might seem to be at fault.

Employers must also be aware of liability risks associated with overtime pay when employees work off-hours on mobile devices, he says. Enterprise mobility management (EMM) tools can be used to check if employees are accessing applications that are not company-approved. But he notes that people already have an expectation of some privacy for the personal information they store on work computers, “and courts and

adjudicators are going to say that I have a greater expectation of privacy over the personal contents of my device that I may use for work purposes."

Finally, when employees leave a company, "oftentimes those departures are not smooth," says Miedema. "The reality is that some employees are not going to cooperate and let the company go through their device and wipe off confidential information." Although devices can be wiped remotely, the employees must first permit MDM software to be installed on their personal devices. "Even if the employee signs a consent," he adds, "when it actually happens and the company wipes the device of personal contact information, they are probably not going to be happy." New platforms like the BlackBerry 10 now enable separate personal and work profiles to be maintained on the same device.

BYOD is a growing global phenomenon, but it is up to each company to develop its own clear BYOD policies, including a framework for resolving issues of security, shared data, and integrity of information – for both employees and employers – to fully benefit from BYOD and to avoid its pitfalls.

Contacts:

Alice Chan, MBA, AMP
Senior Vice President
Mortgage Architects
6505-A Mississauga Road
Mississauga, Ontario L5N 1A6
T: 905-542-9100
alice.chan@mtgarc.ca

Kathryn Kotris, BA, AMP - Mortgage Broker

Vice President of Compliance
Mortgage Architects
3300 Bloor St. W., Suite 3140
11th Floor, Centre Tower
Toronto, Ontario M8X 2X3
T: 416-233-9978
C: 416-540-0406
kathryn.kotris@mtgarc.ca

Adrian Miedema
Partner
Dentons Canada LLP
77 King Street West, Suite 400, TD Centre
Toronto, Ontario M5K 0A1
T: 416-863-4511

Harsh Pabla
CEO
Nanotek Consulting Corporation
81 Zenway Boulevard
Units #1 & 2
Vaughan, Ontario L4H 0S5
T: 888-913-6266
info@nanotek.ca