DLA PIPER

OCTOBER 2014

BYOD IN AUSTRALIA - COOL, CHEAP AND (POTENTIALLY) CATASTROPHIC!

PRIVACY & SECURITY UPDATE

By Alec Christie, DLA Piper Australia

THE ALLURE OF THE POTENTIAL COST SAVINGS OF BRING YOUR OWN DEVICE PROGRAMS IS TOO GREAT FOR MANY AUSTRALIAN ORGANISATIONS TO RESIST.

Not only do the financials of Bring Your Own Device (BYOD) programs look good (the immediate cost savings from the organisation not purchasing the handsets or paying the service plan fees), the organisation is seen as progressive and understanding by allowing employees to pick their own device and avoid the growing phenomenon of carrying two devices, one for work and one for personal use.

In the rush to realise these cost savings with a BYOD program for smartphones and tablets (for example) often overlooked are the numerous and complex risks issues that arise, ranging from information security, general regulatory and privacy compliance through to unhappy employees when the *"wipe"* command is given and the relevant employees lose years of not backed up irreplaceable family photos and videos!

Based on our experience assisting clients in this space and the results of numerous surveys, BYOD smart phones and tablets are the "Achilles heel" of the IT security of most organisations and the technology most often (by a long way) involved in cyber-attacks, data breaches and general privacy issues.

Of course the risks inherent in a BYOD program are not insurmountable or particularly new, often having been dealt with in respect of other parts of the organisation's IT infrastructure and security (eg for laptops and work smart phones). In practice, however, we see many Australian organisations simply not address, often not even consider, the potential risks and issues arising from their BYOD program, let alone implement the appropriate policies or risk management framework. In some of the most extreme cases we have seen BYOD programs run without any involvement of the IT or compliance teams, with no understanding that such devices are part of the organisation's IT infrastructure and therefore no consideration or application of the IT risk management plan or processes or addressing the need for these devices to be treated and managed as part of the organisation's wider IT systems/infrastructure.

Your general security obligations

It is now over six months since the Australian Privacy Principles (APPs) took effect on 12 March 2014 and yet many organisations still do not appreciate their legal obligation under the APPs (in particular APP 11) to "take such steps as are reasonable in the circumstances to protect the [personal] information from misuse, interference and loss and from unauthorised access, modification or disclosure".

The Privacy Commissioner has outlined what these "reasonable steps" are to fulfil this security obligation in a 32 page Guidance (which is currently being updated and we expect will be finalised and reissued soon, with no material changes from the existing Guidance). In our experience at least 40% of the measures suggested by the Commissioner as "reasonable steps" necessary to meet an organisation's security obligations under APP 11 will take most organisations by surprise. Our analysis of the information security obligations of Australian businesses under the Privacy Act can be found in our earlier Update on security obligations.

In addition to the security obligations imposed by the APPs, as explained in our recent Update on cyber risks and the impact on company directors, it is also clear that the security of personal information held by an organisation and management of cyber risks are now part of the duty of care and diligence of a director owed to the organisation. Failure to consider and plan for such at Board level may result in, among other things, liability of the directors for breach of their duty of care and diligence.

So how does your organisation mitigate the risks? What are the key elements of a BYOD program?

First and foremost it is fundamental to know and understand the unique risks posed by a BYOD program (or, for that matter, any technology) to the organisation and determine and prioritise which risks are to be dealt with, in what manner and with what resources. Assuming this risk analysis has been done then the key elements of a BYOD program fall into three broad components:

- **Policies**: A clear (transparent) and comprehensive written BYOD policy outlining the responsibilities of both the employer and the employees participating in the BYOD program and, for the organisation, a risk management framework/policy addressing and managing the security risks of the program.
- **Buy-in:** An agreement (or written acceptance) which employee participants in the BYOD program must sign acknowledging that they have read, understood and will comply with the terms of the BYOD policy.
- **Implementation:** The software/security measures for managing the devices connecting to the organisation's network and implementation and oversight of the risk management framework policy.

Of course the devil is always in the detail. Below we suggest some of the key matters which should be considered and addressed by organisations in respect of these three elements in order to both understand and manage the risks inherent in your organisation's BYOD program:

1. **Who can participate?** For many organisations it will not be appropriate for all employees to be able to participate in the BYOD program. Those employees with access to particularly sensitive or business critical information, information/data of clients of the organisation (for example) subject to restrictive confidentiality arrangements or regulated data (for example APRA licensed financial services organisations) should be required to use an organisation owned device for all organisation communications. A BYOD device should not be allowed to be used in such circumstances/for such employees. In addition, the monitoring of organisation owned devices in Australia is significantly easier than the monitoring/surveillance of BYOD devices under the applicable State laws.
2. **Range of devices**: The flexibility of a BYOD program, which allows employees to choose their own device, is the very thing which can result in the most costs and cause an organisation the most headaches. Does the organisation really want to support all of the multiplicity of hardware and operating system combinations (especially considering the proliferation of Android platforms)? We recommend that the organisation offer a smaller range of hardware and operating system combination options which will be part of the BYOD program and thus supported by the organisation and clearly specify what support will be provided by the organisation. This not only results in the reduction of complexity, it will save on the *"IT learning curve"* and ongoing operational costs (ie number of IT personnel required to support the BYOD program).

3. **Costs reimbursement**: Most BYOD programs contain some form of reimbursement either for the hardware or, more usually, in respect of the service plan fees. It should be clear in the BYOD policy what reimbursement will be made, in what circumstances/when and, of course, tie reimbursement to full compliance with the relevant BYOD policy. We recommend setting a fixed amount for the organisation's contribution and that you resist the temptation to pay/reimburse a percentage of the costs of the device and/or service plan fees. Non-ownership of the device by the organisation does create some concerns with respect to surveillance/monitoring of the device and care should be taken on a State-by-State basis to ensure that the employee monitoring/surveillance laws of each relevant State are complied with.

4. **Employer access (clarity, completeness and consent)**: The cornerstones of any good BYOD policy are clarity, completeness, transparency and the policy's express acceptance/agreement by the employees participating in the BYOD program. It must be clear in the policy that, as a condition of their participation in the BYOD program and among other things, access to the device is given to the employer and that the relevant security measures (including monitoring and a possible data wipe) are included on the device/implemented. Be as clear and complete as possible as to what employer access rights there are (and who "owns" what in terms of apps and data on the device), what security measures will be imposed/implemented and what may happen (ie the consequences) in the case of an event, so there can be no misunderstanding. In addition, it is advisable to inform employees participating in the BYOD program to regularly back up their personal information to ensure that, should an event occur and the device is wiped (for example), they have copies of all of their personal information or, otherwise, such will be permanently lost to them.

5. **Security**: Another essential of any BYOD program is the implementation of appropriate security measures and rules. There are several mobile device management tools on the market which facilitate the security of the user profiles on devices, can remotely lock-out certain parts of or accounts (ie work emails) on the device, create a *"locker"* of sorts for the secure storage of work related data and files, handle encryption keys between the device and the organisation's network, enhance the strength (ie force the use) of user passwords on the device and/or enable remote wiping of either work related files or, more usually, the entire device in the event of loss or theft. The consequences to employees of circumventing any of the security measures on the device or not following the security rules should also be clearly spelt out.

6. **Rules of use**: Ensure that your acceptable use/IT use policies apply to the BYOD program and devices (and clearly remind participants of this in the terms of the BYOD policy). You may also wish to include additional BYOD specific rules (eg, from recent experience, no use of the device by any children, no lending your device and password to others, including family members), including if any specific applications or particular type of applications are not allowed.

7. **Exiting employees**: The organisation must have a process in place for removal of all of the organisation's data from the device (usually with delivery up of the device for a certain period for such purposes) on the exit from the program or the organisation (for whatever reason) of any BYOD participating employee. In addition to the readily identifiable work files, other work data/information should be removed (for example contacts included in the employee's personal contacts on the phone, if they are also work related contacts, should be removed). Again, clear, complete and transparent wording in the BYOD policy as to what may be done/removed by the organisation on exiting the BYOD program or the organisation will greatly assist the exit process.

Conclusion

Despite the sensational title of this Update, BYOD programs do not have to be catastrophic for your organisation if implemented in a considered and planned manner, taking into account all relevant risks and issues (including treating the devices as part of the organisation's IT infrastructure) and if appropriate policies and risk management are implemented.

Our concern is not that BYOD programs cannot be done properly (with minimal/acceptable known and

managed risks) but that, in practice, many Australian organisations are simply not doing so. Unfortunately, rolling out a BYOD program without an appropriate policy or considering and managing the inherent risks is currently the norm for Australian organisations, not the exception.

Please do not hesitate to contact any of our dedicated privacy team if we can assist with your BYOD program or any other privacy related matters.

MORE INFORMATION

For more information, please contact:

Alec Christie
Partner
T +61 2 9286 8237
alec.christie@dlapiper.com

Contact your nearest DLA Piper office:

BRISBANE

Level 28, Waterfront Place
1 Eagle Street
Brisbane QLD 4000
T +61 7 3246 4000
F +61 7 3229 4077
brisbane@dlapiper.com

CANBERRA

Level 3, 55 Wentworth Avenue
Kingston ACT 2604
T +61 2 6201 8787
F +61 2 6230 7848
canberra@dlapiper.com

MELBOURNE

Level 21, 140 William Street
Melbourne VIC 3000
T +61 3 9274 5000
F +61 3 9274 5111
melbourne@dlapiper.com

PERTH

Level 31, Central Park
152–158 St Georges Terrace
Perth WA 6000
T +61 8 6467 6000
F +61 8 6467 6001
perth@dlapiper.com

SYDNEY

Level 22, No.1 Martin Place
Sydney NSW 2000
T +61 2 9286 8000
F +61 2 9286 8007
sydney@dlapiper.com

www.dlapiper.com

AGC/TAH/00001/0510240/AUG/1202188846.1