Should small businesses be jumping the BYOD ship?

Bring your own device (BYOD) is on the wane as companies move towards a tighter corporate provisioned model that embraces the consumerisation of IT in a more controlled manner.

A recent study by Forrester Research revealed that 68 percent of Australian and New Zealand enterprises with 1,000 or more employees have a corporate provisioned model where employees can either choose a smartphone from a company-approved list, also known as CYOD, or take a more traditional approach and have the company issue one directly with no choice at all.

The theme is consistent amongst smaller businesses as well, with 51 percent of ANZ small and medium enterprises (SMEs) that have 20 or more employees utilising a corporate provisioned approach, versus 48 percent opting for BYOD.

BYOD has also fallen out of favour amongst businesses in the wider Asia-Pacific region, with numbers from IDC's latest survey showing that 25 percent of organisations having headcounts of between 50 and 249 people are BYOD only. That figure falls to just 18 percent for companies with a 1,000-plus headcount.

However, it's important to note that BYOD remains dominant for a large majority of small businesses with less than 20 employees.

So why exactly has BYOD declined in popularity for larger businesses, and is this something that small businesses should be concerned about?

For a large company, the need for a corporate provisioned mobility strategy like CYOD comes down to two main drivers: Security and cost.

A recent report by analyst firm Gartner categorically declared the end of the era of BYOD, stating: "There is no way for IT to assume full responsibility of securing and managing devices without ownership."

Integrating an organisation's infrastructure resources onto a mobile platform can be done tighter and more securely under a CYOD program, where a range of devices are put through corporate IT testing and certification to ensure compliance. The rise of private cloud deployments and hybrid cloud infrastructures where firms

have to secure every device that can connect to their internal cloud computing network is a good example of this.

Under BYOD, however, employees can access the corporate cloud and the sensitive data stored within them from non-company-sanctioned devices, which poses a potential security risk that many CIOs simply aren't willing to gamble on.

Regarding cost, while it was initially thought that BYOD could drive down the cost of acquisition, this was only part of the story. An increasing number of enterprises are realising that the total cost of ownership is actually higher with a BYOD strategy.

There are several factors driving up costs:

- Enterprises lose the ability to collective bargain with telcos for lower-cost plans, which can result in reimbursing a higher amount of telco-related expenses and higher roaming/data costs.
- The 80-20 rule: In a corporate-owned model, IT can spend 20 percent of their support and address 80 percent of the users, whereas for BYOD, 20 percent of users will take up 80 percent of IT's mobility support, which further drives down efficiency.
- For larger enterprises, it's all about standardisation. Standardising mobility creates stability, efficiency, and a platform to build on. As long as employees are getting the devices they want to use, do they care who owns it? The answer is usually no.
- Apps and data are much more important than the devices. With larger enterprises, device management is becoming standardised, which makes deploying apps and data easier. It's becoming less about what or whose device to manage, and more about how to provision and secure the apps and data.

However, the issues of security and cost associated with BYOD don't really apply to small businesses.

Small businesses don't usually have all these established process-driven models when it comes to procurement, support, and cost management. To them, mobility is a way for their employees to be more mobile, productive, and flexible. The reality is that small businesses are using BYOD to produce real, transformative results for their businesses.

A business with 10 staff members is less likely to have a private or hybrid cloud infrastructure, and is more likely to use public cloud services. Small businesses tend not to build internal business apps, and instead utilise pre-made, off-the-shelf, cloud-based apps that run on any device -- so there's much less need for standardisation.

And while there may not be a cost-saving benefit in BYOD for large businesses, the same cannot be said for small businesses. The fact that the purchase and maintenance of the BYO device is at the expense of the owner of the device makes a significant impact on the bottom line of a small business.

Unless the small business operates in an environment where employees handle highly sensitive data, there is simply no tangible benefit for scrapping BYOD in the workplace for a more controlled option. That said, as small businesses get larger, by definition so too will the importance of data security, employee privacy, support, and cost, at which point a shift towards CYOD might be a better solution.

At the very least, what the overwhelming adoption of CYOD amongst larger businesses tells us is that a pure-play BYOD model might not be the best strategy for business growth in the long term, and that a revisit of the company's mobility management approach would be wise sooner rather than later.