The Accidental CIO | Rob Livingstone

Don't let BYOD become bring your own disaster

How to get the executives to see why users cannot do whatever they want with their mobile devices.

Shadow IT in one form or another is here to stay, and when it comes to BYOD, IT leaders that have an open and engaging approach to this challenge will most likely win the opinion war.

For those IT leaders still grappling with managing BYOD and its risks and security issues, here are some simple steps to help get you on your path to ensuring BYOD doesn't end up in disaster:

STEP 1: Print out a copy of the draft paper by the US National Institute of Standards and Technologies (NIST), entitled *Recommended Security Controls for Federal Information Systems and Organisations [SP800-53]*, which can be downloaded at *csrc.nist.gov/publications/PubsDrafts.html*.

STEP 2: Read the document and highlight the parts that are relevant to you and your organisation. The core information is contained in the first 18 pages of the 29-page document. If you think you have got the BYOD issue all sorted, this document may make you reassess and adjust your position – after all, volatility and change is the norm.

STEP 3: Put BYOD on the next monthly executive team meeting, if you have not done so already.

Pre-issue a succinct BYOD position paper that you have prepared and is relevant to your business and security posture. This should be a business document stripped of technical jargon. Ask a family member or a friend to proof read it – preferably someone who is not in IT. If they can understand it, then it's good to go and be read by the executives.

This is an important step in:

- Managing expectations and opinions on BYOD at the senior management level in your organisation
- Ensuring that any subsequent policies and other mandates are fully supported by all executives
- Assigning accountabilities on the policy settings to those in the organisation, with expert guidance from you.

Remember:

- State what is BYOD and explain why it's important to your organisation
- Summarise the benefits of BYOD, including a high level cost/benefit assessment that is relevant to your situation, emphasising that it requires active management
- Summarise the key business risks to the organisation
- State your recommended position. This could be a draft policy, a series of 'next steps'.

STEP 4: Seek ratification for a course of action that you feel appropriate. Suffice it to say you should be well prepared to discuss the issues, hear concerns and adjust your position accordingly. The cost/benefit of various security measures, as well as the acceptance of the residual risks, mostly rests with the business. As long as your explanation of these risks by you is comprehensive and rigorous, and these decisions are on the basis of sound, unbiased advice, you should be able to sleep well at night.

Without the visibility and support of all executives across the organisation, it will be a constant challenge for IT leaders to keep having to explain why users cannot do whatever they want with their mobile devices. This could leave you being constantly on the defensive, rather than proactively managing and guiding the organisation through the enterprise IT minefield.

At the end of the day, if you can ensure that the key executives appreciate that the organisation's reputation and brand are at stake, not yours, then the war will largely be won, not only for BYOD, but also for the other side effects of Shadow IT.

Rob Livingstone is a respected and experienced CIO, with more than three decades of industry and ICT experience. Over the last 16 years, he has held the CIO role at several multinationals, most recently Ricoh. He is the owner of Rob Livingstone Advisory and a fellow of University of Technology, Sydney. Rob delivers the Pathways Advanced and Business ICT Leadership programs in conjunction with the CIO Executive Council.