How can SMEs harness 'Shadow IT'?

By Brian Timperley

1 Nov 2018

For many of us, the term 'Shadow IT' instantly evokes images of nasty ghouls lurking suspiciously behind servers and computer screens - waiting for the moment to cause mass cyber destruction.

The true meaning of Shadow IT, however, is a little less dramatic. Put simply, it refers to the use of IT-related software or hardware by a department or individual without the knowledge, control or explicit permission of the organisations IT department.

Perhaps the most obvious current example is the general use of WhatsApp – people have become so accustomed to using this messaging platform outside of the office, that using it in the workplace (for business communications) is almost second nature. Another commonly used tool is the file storage service Dropbox, which employees often choose to use instead of more ‘official’, commercial platforms.

Brian Timperley, joint MD of Turrito Networks & Dial a Nerd

So what’s the big deal? Where does the ‘Shadow’ part come in, and why the concern?

For business owners, and particularly those in the SME space with fewer IT resources, Shadow IT can present a significant security vulnerability. According to research firm Gartner, by 2020, one-third of successful cyber attacks experienced by enterprises will be on their Shadow IT resources.

In other words, Shadow IT represents a rather big black hole in most enterprise security strategies today. Numbers released from Cisco Cloud Consumption engagements have revealed that large enterprises, on average, use over 1,200 cloud services— and over 98% of them are Shadow IT. For SMEs, this percentage is likely to be similar, if not even higher.

Source: pixabay.com

Beyond the obvious security risk, Shadow IT also causes headaches when employees use applications on the network without paying licensing fees – which can lead to hefty fines if the apps are being used commercially.

Embracing the 'dark side'

Remember when your grandma said “Keep your friends close, and your enemies closer”? This, in a nutshell, is the best way to approach Shadow IT today. As Gartner and many other analysts have pointed out, Shadow IT is a reality that every business must quickly learn to embrace, and IT Departments must know it exists and understand what lurks in these shadows.

Indeed, the presence of Shadow IT arguably boosts productivity, employee engagement, and overall employee happiness. This is simply because people become accustomed to using certain applications and platforms in their homes and in social scenarios, and naturally want to stick with those tools in the workplace. Often, these tools are more accessible and easier to use than enterprise solutions, and are usually free. To return to the WhatsApp example, while it’s not your typical business tool, it’s arguably more effective with remote staff than some paid-for business communication tools.

The first step towards embracing Shadow IT is to understand how - and more importantly why – certain tools are being used. Most often, employees are just trying to get their work done smoothly and more efficiently.

If the Shadow IT tools they are using are that much easier than the tools provided by the organisation, the IT Department must consider whether they are in fact providing the right tools in the first place.

Source: pixabay.com

The next step is to identify whether or not these tools present a security risk. These assessments need to be carried out regularly, and thoroughly. Finally, if and when certain Shadow IT tools have been identified as more powerful and capable tools than those currently deployed, then it's time to consider making these (or similar tools) official, and bring them out of Shadow IT when possible.

Notably, if an operating system such as Windows could pick up installed applications and make it reputation-based (similar to the Apple App Store) it would potentially make Shadow IT more manageable. Business owners can also explore new BYOD (Bring Your Own Device) policies. Today, some organisations segment their networks so that these devices have their own network (and won't negatively impact the business).

As new, slick technology tools and applications enter the consumer space (as they invariably do) savvy business owners and managers can ensure that these innovations work for – not against – business growth and productivity…

ABOUT BRIAN TIMPERLEY

Brian Timperley is managing director and co-founder of Turrito Networks and managing director of Dial a Nerd.
- #BizTrends2019: SA businesses moving closer to data-driven decision making - 7 Jan 2019
- SA businesses gains access to key global platforms in 2018 - 7 Dec 2018
- How can SMEs harness 'Shadow IT'? - 1 Nov 2018
- The connected business society - 24 Jun 2016
- [BizTrends 2016] IT's changing of the guard - 18 Jan 2016

View my profile and articles...