CIOs vs. consumer technology: it's time to change strategy

By Sumash Singh

6 Oct 2015

Every day we hear about new data breaches or data losses, with high-profile cases bringing data security into the mainstream news agenda. There is no denying that the role of today's CIO is increasingly complex and unpredictable. This is partly thanks to the proliferation and seemingly uncontainable nature of new technology solutions. One such example is the use of file sync-and-share (FSS) solutions in an enterprise setting, a cause of many data breaches.

©Dmytro Sidelnikov via 123RF

Opening up Pandora's box

With the rapid adoption of FSS solutions for personal use, it is increasingly becoming standard procedure when accessing, storing and sharing business information in the workplace. Unfortunately, as with most technology built with consumers in mind, FSS solutions fail to provide businesses with the security they need for protecting critical business information. It has opened up a Pandora's Box for security and data loss challenges because they're rarely managed by, or even visible to, IT departments.

In recent years, CIOs have exhausted much of their energy campaigning against the use of consumer technologies in the enterprise, and yet are increasingly unaware of what's happening with technology in their own organisations and have little control of what is being downloaded or transferred across them. Shadow IT is simply not going away.

The fact is the approach of trying to restrict the influx of consumer technology entering the enterprise has been unsuccessful. Now this is not to say CIOs should take the tact of 'if you can't beat them, join them', but it is necessary for CIOs to change strategy and instead position themselves as the enablers of these technologies, rather than the blocker.

So how can you ensure that data shared through services such as OneDrive, Dropbox and similar solutions remains visible to IT, backed up, and fully searchable for use by end users and for eDiscovery purposes?

The following guidelines are essential to ensuring your workplace supports FSS:

• **Accept shadow IT behaviour is taking place:** Don't ignore rogue file sharing behaviour. According to a research report by Osterman Research, 68% of business users were storing work-related information in a personally managed FSS solution - without visibility or approval from IT.

• **Listen to your colleagues:** By learning how and why staff choose to use FSS on the job, you can better understand how IT can encourage this continued collaboration platform with the support of additional data governance and security measures such as encryption, backup and eDiscovery. It will also enable IT to better choose which applications it rolls out across the company, in order to meet staff requirements.

• **Promote easy-to-use services:** Remember that one of the most important features of FSS services is the user-friendly interface and quick deployment. Look for a tool that combines the functionality, security and scalability required for an enterprise solution with the ease of use of a consumer-class FSS. Some solutions offer a virtual folder that acts as a "personal cloud" so that staff can freely collaborate and share work-related files just as they would via FSS solutions, but without the security risk.

• **Take responsibility:** FSS integration into endpoint data protection solutions needs to be an IT responsibility. By putting in place the correct guidelines and approval processes, the IT team can finally put away the rubber 'no' stamp and be the department that colleagues look to for the tools they need and want.

• **Keep your options open:** Users choose FSS to increase productivity, collaborate with colleagues and backup files. As such, be sure you can continue to support a wide range of devices and third-party applications when you implement that extra layer of protection. It's important not to be limited to a specific platform or ecosystem either, so make sure users still have access to the same features across all devices.

Following these guidelines will reinstitute the IT department as the guardian of consumer technology solutions in the workplace, and therefore IT teams can ensure that they can recover, access and use company information no matter where it resides - while reducing costs and risk. In much the same way as the shop assistant lives by the saying 'the customer is always right', CIOs must now recognise that they should be guided by their staff. By learning from the habits that work outside the enterprise, it is possible for IT to provide a smart complement, and/or alternative, to existing solutions, while still adhering to corporate data management best practices.

ABOUT SUMASH SINGH

Country manager at CommVault
- CIOs vs. consumer technology: it's time to change strategy - 6 Oct 2015
- The rise of the chief data officer - 1 Oct 2015
- Designing a cloud that meets your business requirements - 7 Sep 2015
- Safe cloud computing starts with sound information security practices - 22 Jul 2015

View my profile and articles...