Adapting to change in a virtual world

By Bryan Balfe   5 Jun 2014

It should come as no surprise that the biggest technological impacts on IT departments in 2013 were mobile and big data. Both issues also dominated conversations in the storage arena last year and with employees now increasingly working remotely, it's highly likely that 2014 will see more and more organisations struggling to manage large volumes of data.

Equally challenging will be providing secure access to, and protection of, potentially sensitive but undoubtedly valuable information generated on a growing number of mobile devices.

With approximately one-third of the global workforce predicted to be mobile by 2015 (IDC, Worldwide Mobile Worker Population, 2011 to 2015), it's clear that the Bring Your Own Device (BYOD) movement has created massive market demand for end-users to be able to access data from any device quickly and to benefit from collaboration and knowledge sharing regardless of their location.

The mountain of data now residing on mobile devices, however, is forcing companies to rethink how they securely capture, store and retrieve data in order to derive more value from it - whilst remaining compliant. Indeed, Gartner has recently suggested in its report entitled BYOD is an applications strategy, not just a purchasing policy (November 2013) that what is needed is "global class" computing - "an approach to designing systems and architectures that extends computing processes outside the enterprise and into the cultures of the consumer, mobile worker and business partners".

Needs to be addressed without hesitation

That said, it also appears that too few organisations have either devised or implemented comprehensive strategies to support these mobile workers, or are yet to put in place measures to ensure regular back-ups from mobile devices as a minimum. Protecting access to sensitive data and providing an alternative to storing company data on local or removable devices is critical and needs to be addressed without hesitation.

In South Africa, organisations struggled to adapt their processes to accommodate BYOD; however, in the last year, we have seen some progress made in this area. Security is still a concern as BYOD brings much uncertainty. Many businesses focus purely on data that is "on the move" and not the security of the device. Although local companies are currently trying to accommodate BYOD, there are still many challenges to tackle.

There is a lot of reliance on cloud services like Box and Dropbox to gather and share information across an organisation, which itself presents a number of IT headaches for companies. Trying to make a consumer product work for the enterprise inevitably means that mobile management remains outside the IT department's awareness and control, and, as such,

valuable corporate data is left unprotected. From another perspective, it's essentially "lost" to all employees across the organisation for the purposes of collaboration and knowledge sharing.

Currently, local organisations are not discussing third-party cloud-storage solutions and the role they play with BYOD. It is essential for legal, compliance and finance executives to be fully aware of how much corporate data is currently being stored in these cloud tools. I believe these executives should work with the IT department to formulate policy and be part of the discussion around risk versus productivity.

So while the emphasis in 2013 may have been on creating modern data management strategies, the priority for 2014 now has to be the synchronisation of files and preparation for automated retention methods to reduce the risk of data loss.

It makes data fluid, not siloed

The biggest single benefit of automated and continuous file and folder synchronisation is that it makes data fluid, not siloed. It supports different environments and operating systems (OS) and provides guaranteed access either to old documents indefinitely or to the most recent files instantly, regardless of the device on which they were created.

However, given that synchronisation is different from traditional back-up, what is also needed in order to encourage the widespread adoption of a central corporate repository are centrally defined yet automated processes that improve mobile data protection without any involvement from the user. IT needs to regain sight and control of all remote offices, and mobile devices, and to be able to provide a back-up service that reaches all areas of the network in an instant.

This is perhaps the only way, after all, to ensure that IT has the latest version of every user's files at any given time. Just as important in this data-focused age is the delivery of self-service access to protected files and emails 24/7. Fast-restore times and intuitive, role-based search capabilities are now expected by users - across all enterprise data - as standard in order to simplify search and e-discovery. Submitting a ticket and waiting for IT support is no longer acceptable. Any delay in access only increases the likelihood that employees will return to the high-risk, consumer file-sharing tools and ad hoc cloud back-up services.

It's also important to note at this time, however, that enterprises are becoming more and more comfortable with the security and scale of public cloud resources from big providers. Rather than burden their networks, they are instead opting to use this solution when using a heavy application like SharePoint, Oracle or SAP. This potentially means that we are likely to see private cloud growth coming from industries like finance and health care, where there are significant compliance or security issues and where there is a need to know that data hosted onsite is treated as mission critical.

Move data seamlessly

Organisations are beginning to investigate the benefits of integrating their data management solutions with cloud platforms, enabling them to move data seamlessly from an on-premises data centre to infrastructure-as-a-service (IaaS) from leading cloud providers. The challenge is to harness automated, content-indexed data collection, protection, access and retrieval from a central console with low-cost-cloud storage for data archiving. This has the potential to enable organisations to add storage capacity to keep pace with data growth without placing an additional burden on the IT department. It also makes it possible for organisations and service providers to leverage cloud services efficiently to meet service level agreements (SLA) and budgetary requirements.

ABOUT BRYAN BALFE

Channel Manager at CommVault in South Africa
▪ Understanding data sovereignty and its importance to your business - 22 Sep 2015
▪ Controlling data risk in the BYOD onslaught - 19 Aug 2015
▪ What enterprises can learn from the MSP revolution? - 13 Aug 2015
▪ Warning signs your archiving strategy is not geared for the future - 24 Jul 2015
▪ Driving forces behind cloud computing - 22 Jun 2015

View my profile and articles...