READERS' LETTERS

Datacentre decisions

Stuart Sutton, CEO, Infinity SDC

The recent acquisition of Telecity by Equinix may have been one of the largest datacentre acquisitions to date, but has it thrown the industry into disarray? I don't think so. The datacentre industry is booming – demand for the cloud services needed to stream consumer and business applications has increased the opportunities for all providers.

However, there are three substantial considerations. First, the types of contracts some vendors operate within are very blinkered. Fixed terms stifle any type of flexibility and limit customers from broadening a partnership in any way. Sadly, the providers know they have the services needed, so many customers have their hands tied behind their contractual backs.

Second, some existing Telecity customers have already made the choice to collocate with two different providers for a number of reasons, including business continuity and resilience. The time it takes to make these decisions will be eradicated with this deal, if they are co-located with the same provider. The result is that new customers will have a limited choice when sourcing a datacentre partner, which may encourage them to consider other providers.

Finally, an issue prevailing across every continent, is data sovereignty. The key advantage of an EU hosted datacentre for a global business is the prohibition on personal data exports falling away. Using a service in the EU eases regulatory hurdles so clients can better ringfence the personal data of the business from requests for disclosure by, for example, US administrative or enforcement bodies.

However, if EU clients wish to avoid the risk of their data being vulnerable to requests by US administrative or judicial bodies, the storing of data in the EU needs to be combined with the precaution of using a wholly owned EU datacentre provider (or indeed a datacentre provider that is not a subsidiary of a US parent).

The global landscape for data privacy laws (outside Europe) are changing at pace, and while we await further maturity of interpretation for many of these new laws, we should be a little more cautious as to the long-term implications of consolidation.

It's time data protection was taken more seriously

Paul German, vice-president EMEA, Certes Networks

In response to a recent survey by LogRhythm, I find it shocking that almost half of organisations that have suffered a data breach took more than four months to detect the issue. Businesses are still not doing enough to protect their networks from today's threats.

The immediate reaction – the focus on fixing the threat detected – is, of course, essential, and is something that businesses must begin to put into practice. A three-month lag between detecting the problem and mitigating the risk is frankly unacceptable. Quite simply, even just a week of unfettered data exfiltration can equate to millions upon millions of records.

As well as placing importance on fixing threats once they occur, it is also vital for organisations to concentrate on preventing attacks in the first place and, most importantly, containing breaches once they happen.

The real imperative is that the security architecture as a whole must be fixed; it has not evolved at the same speed as the new world of digitised data and the borderless applications that have been hacked in every major breach case. The common security architecture is still built around the antiquated notion that a firewall can keep the 'bad guys' out. If any enterprise application is being shared with any external party, then even the most advanced next-generation firewalls cannot guarantee that the application is safe.

The need is for architectures to adapt to the new world of applications by ensuring that network segmentation and application isolation can be applied across all network environments, both external and internal. User access control policies must then be applied and enforced in real-time, across all users and all applications both inside and outside the traditional firewalled perimeter.

The time for the industry to recognise that a fresh approach is needed is now; if companies wait for another global data breach before making changes it will purely be too late. ■

> "I find it shocking that almost half of organisations that have suffered a data breach took more than four months to detect the issue"
> Paul German, Certes Networks

› **Send your letters and comments to squicke@techtarget.com**

The pressing need for better storage

Tarkan Maner, CEO, Nexenta

In June, an independent report, commissioned by home secretary Theresa May, ruled that surveillance activities by the security services should be maintained and agencies should have the right to monitor phone and internet use. The findings, which were delivered by the report's author, David Anderson QC, provide the foundations for the Investigatory Powers Bill which will come into effect in the autumn. While it will certainly be taken up by privacy campaigners, who believe the bill will give the powers that be more scope to 'snoop', one practical challenge that has so far been ignored is how traditional storage systems will cope with the avalanche of data on its way.

In this digital world, data is the new currency. Companies are collecting more and more information about their customers – from the websites they browse to the type of bread they buy – in the hope that this seemingly innocuous data can be turned into actionable business intelligence. However, despite the industry continuing to innovate, churning out big data tools capable of harnessing and getting the most out of this growing pool of information, one thing is abundantly clear – there is a ticking storage clot in the system.

Too many businesses are still reliant on traditional storage that is not flexible or scalable enough to accommodate this incoming surge in demand capacity. As such, amid the hype, it is the role of the channel to educate its partners about the next generation of software-defined storage (SDS) technology. By streamlining the data flow, and hardware agnostic by design, businesses eager to embrace big data and capitalise on all it promises will be able to do so in a sustainable, affordable and long-term fashion.

CONTACTS

MicroScope
2nd floor, 3-4a Little Portland Street
London W1W 7JB

WEB
www.microscope.co.uk

GENERAL ENQUIRIES
Office Manager Monique Robinson
020 7186 1401

EDITORIAL
Editor Simon Quicke
020 7186 1412 squicke@techtarget.com
Senior reporter Sean McGrath
020 7186 1477 smcgrath@techtarget.com

Production editor Claire Cormack
020 7186 1417 ccormack@techtarget.com
Senior sub-editor Jason Foster
020 7186 1420 jfoster@techtarget.com
Sub-editor Ben Whisson
020 7186 1478 bwhisson@techtarget.com
Sub-editor Jaime Lee Daniels
020 7186 1417 jdaniels@techtarget.com

ADVERTISING
Sales director Brent Boswell
07584 311889 bboswell@techtarget.com
Account manager Martin Upson
020 7186 1451 mupson@techtarget.com

EVENTS
Events manager Tom Walker
020 7186 1430 twalker@techtarget.com

MicroScope is produced monthly by TechTarget, 3-4a Little Portland Street, London, W1W 7JB, UK.