Bob Tarzey
Quocirca
19 November 2007

Written as background to a presentation to be given by Quocirca at the Qualys CSO Interchange in London, 27 November, 2007

Security consequences of greener IT

Quocirca analysts are encouraged to think about the broader consequences of the information technology (IT) advice that they offer. So, regardless of an analyst's specialisation or the focus of a particular report, questions such as "what are the security issues?" or "is there an open source angle?" are frequently addressed. In the last few years another broad ranging topic has been added to the list "what is the environmental impact?" However, some questions bring these broad themes together, and Quocirca was asked one recently – "what are the security consequences of greener IT?"

Having thought the question over, Quocirca has come up with an answer. There are two broad themes that affect the job of chief information security officers (CISOs) if businesses are serious about "greening" their use of IT. The first is a positive one: on the whole more IT infrastructure should end up housed in more resilient and secure data centres; the second is more negative from the CISOs view point at least: businesses will have to accept, indeed embrace, even more open and flexible use of IT, often requiring access over the internet.

Greening IT requires three issues to be addressed: facilities, infrastructure and usage.

By facilities we mean the locations where IT is used – data centres, offices and in the field. The last two are harder to control, but a data centre has the potential to be managed very efficiently where there is a will. 21st century data centre design is all about efficiency and, fortunately, that can also mean green. Efficient cooling, minimising energy requirements and reuse of heat have been covered in other articles by Quocirca. All save power costs and reduce CO2 emissions. A lower carbon footprint is good – but what about zero carbon?

To be clear, zero carbon is different from carbon neutral. It means deriving all energy requirements from sustainable power sources, not just offsetting those of dirty power derived from fossil fuels – coal, oil and gas. Putting nuclear power to one side for now, this means hydro, wind, solar, tidal and geothermal power. Making use of such power sources is already a reality.

Google is building new data centres in remote locations near hydroelectric schemes. Yahoo is talking about locations such as Switzerland and Iceland. A UK co-location provider, Centrinet, has a carbon-zero data centre in remote and windy Lincolnshire. These data centres are located close to power generation as it is more efficient to transmit data than electricity and there is less competition from other human activity. In the future – who knows – solar powered data centres in the Sahara?

This is all possible but the remoteness of such zero carbon power generation locations makes them a long way from users whoever they are. So whilst such locations are quite easy to make physically secure and will provide a resilient infrastructure for housing IT, the data they generate will have to be transmitted over long distances. For reasons we shall come to, this journey will often be over the internet.

Great – so long term there is potential to make data centres zero-carbon. There has also been much coverage of how to make the infrastructure housed within more efficient using consolidation, virtualisation and so on. But surely there is as much power used by IT infrastructure scattered around offices and carried by employees in the field. Not much can be done about that, surely? Well, yes, quite a bit actually. First, power management applications can help in offices, although in the field you do have to rely pretty much on the common sense of employees (often problematic – agreed). But there is plenty of scope for consolidating infrastructure into the "carbon friendly" data centre.

Many workers only use IT in the office and can be served by thin-client computing or blade PCs run out of data centres, considerably reducing the use of power at the desktop. Branch office computing requirements can also be served out of data centres, reducing power usage and keeping network "heavy lifting" between "clients" and "servers" local to the data centre, rather than across wide area networks (WANs). Good news for the CISO here – more infrastructure in a secure and controlled environment and less ad hoc access over WANs. For offices workers and many branch workers the network used will be a private one, so not too much extra concern about the remaining network traffic.

To some organisations, getting access to high quality data centre space may sound expensive. But it need not be. First it is possible to procure such space from co-location providers, like Centrinet, Telehouse Europe or Netcetera, or just rent hardware provided by managed service providers who use co-location facilities like Rackspace or NTT Europe Online. But an increasing popular alternative is to turn to software-as-a-service (SaaS) vendors who provide subscription-based access to applications ranging from CRM (e.g. salesforce.com, NetSuite, RightNow) to IT security (e.g. MessageLabs, Google/Postini, Qualys). All SaaS providers have to use robust well managed data centres facilities to underpin their business model.

The real security headache for CISOs is around usage outside of the office. This is not so much about what employees do with IT but the fact that any business going green needs to open its IT infrastructure to a broad spectrum of external users. Unlike other industries that are lambasted for their CO2 emissions, such as air travel and road transport, as we have seen, IT usage already has the potential to be low or zero carbon. So rather than being an environmental pariah, IT can be used to drive initiatives that green the business in other areas.

Collaborative applications like web and video conferencing are becoming more and more widely used and, whilst claims that these reduce the overall carbon footprint of a business need to be substantiated, their use is a direct alternative to travel. But such collaboration needs to be with suppliers, customers and other business partners, not just between employees. For this to happen requires open access over the internet.

Business processes such as supply chain management and distribution are increasingly being opened up for direct access by businesses to external entities. This helps ensure the efficiency of the transportation and storage of goods. But again this requires wide ranging access to IT over the internet by third parties. And then there are employees working flexibly, field service engineers clocking in remotely using handheld devices, sales staff logging orders direct from customers' sites and call centre workers based in their own homes. All have the potential to make a business greener, especially if the applications themselves are run using low or carbon facilities and infrastructure.

So, in answer to the question initially posed, the greening of IT means housing as much infrastructure as possible in secure data centres that will become increasingly remote and potentially zero-carbon – this introduces more control, security and resilience. But it also means providing wide ranging access to applications housed in such facilities, often over an inherently insecure network – the internet. But, unlike many other activities that are hungry for power, well managed IT has the potential to give more back to the environmentally aware business than it takes.