Global Digital Infrastructure Trends

Findings From the 451 Alliance

September 11, 2015

IN THIS ISSUE:

Quick Snapshot: Today's Newsletter

Public Wi-Fi Security. With more people randomly accessing open Wi-Fi networks, the public is vulnerable, and it's putting the businesses they work for at risk. What can be done to protect against rogue networks masquerading as free Wi-Fi?

Cloud Services. A recent 451 Research ChangeWave survey looked at consumer usage of cloud storage services – including competition among the major vendors and customer satisfaction ratings.

Microsoft's Quest to Cut Carbon. In 2012, Microsoft imposed an internal tag on its carbon emissions – and has used the resulting carbon fees to support a range of energy and datacenter environmental initiatives. But how well is it keeping the company's energy costs and carbon emissions under control?

Health Info and IaaS. How can a strong vendor-client partnership lead to massive system-wide transformation? Here's a quick snapshot on how Cambridge University Hospitals shifted from a fragmented, paper-based environment to one that accesses all data via IaaS. It's a revelatory story.

I. Public Wi-Fi Security: Who's Watching Whom?

Wi-Fi networks are vulnerable. While this comes as no surprise to anyone working in security, it's now putting members of the public and the businesses they work for at risk.

From people carelessly agreeing to terms and conditions to randomly accessing any open network, the problem has become rife as millions upon millions of devices are connecting to public Wi-Fi in the smartphone age.

But just as mobile device management became the workplace solution for BYOD, similar solutions are needed for mobile security in the public domain.

The good news is that tools are emerging to help people and enterprises reduce the risk.

Wireless Networks in Public Places

Since the advent of the smartphone, the presence of wireless networks has increased massively in the public arena, from the more traditional offerings in coffee shops, to supermarkets, bars, retailers and even airplanes – all of them bent on offering access to the Internet and online apps.

The spread of these networks puts not only the public at risk, but enterprises as well. Corporate employees are part of the public after all, and they too are tapping into open Wi-Fi networks.

In response, security tools such as virtual private networks (VPNs) are being built into the operating systems of laptops, and more recently mobile devices. But is this enough?

Far too often, user validation is limited to 'this looks okay to me.' While various awareness projects – such as the Cyber Streetwise campaign in the UK – have done a good job of raising awareness of cyber issues to the public, simply knowing which Wi-Fi networks are safe to use is arguably the weakest security model in the industry.

Research conducted a few years ago at an Infosecurity Europe exhibition further underscores the seriousness of the problem. Within just a few hours, 143 attendees connected to the fake wireless network 'Free Infosec Wi-Fi.'

So in a world where the common belief is 'Wi-Fi is free,' what can be done to better protect people from being snared by rogue networks masquerading as free Wi-Fi?

When it comes to privacy, VPNs provide a level of protection against casual eavesdropping, and there are endpoint management tools for laptops that only permit access to the VPN gateway when a host is on another network.

Thus, while you can't educate an entire nation, Microsoft does offer VPN software as part of its operating systems, and there are options available from Citrix, Barracuda, LogMeIn, Palo Alto Networks and Dell SonicWALL, to name a few.

From an enterprise-protection point of view, another option is network access control (NAC), whereby the management of enterprise mobile device security is better achieved. In particular, managing the wireless connection of devices with preset security conditions better protects against unwanted infections caused by mobile devices.

There are other technology options in this space. For example, ForeScout has a product that doesn't require 802.1X authentication for enterprise NAC and extends through wireless networks. Further options are available from Cisco and Aruba Networks.

Yet a certain amount of business exposure remains given the ubiquity of free public Wi-Fi, the need for widely available connectivity, and the fact that not all network communications may be amenable to VPNs.

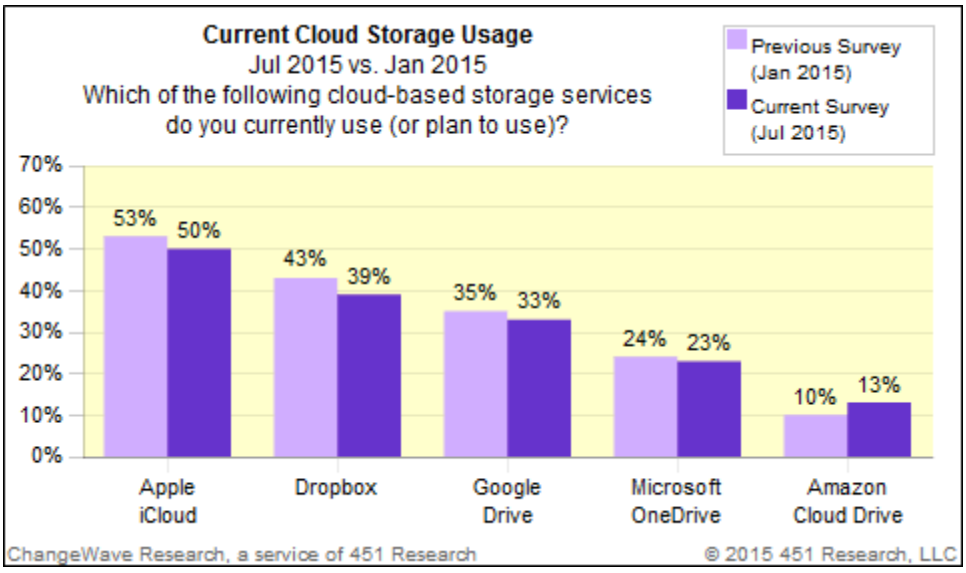
Cellular networks may someday displace Wi-Fi as the option of choice (indeed, personal hotspots are already common in the form of mobile device tethering). But for now, enterprises face hurdles in extending protection across poorly validated public networks – and significant business risks remain.

II. Consumer Cloud Services: The Battle to the Top

A recent 451 Research ChangeWave survey of US consumers focused on their usage of cloud storage services – including the vendors they use and their satisfaction with them.

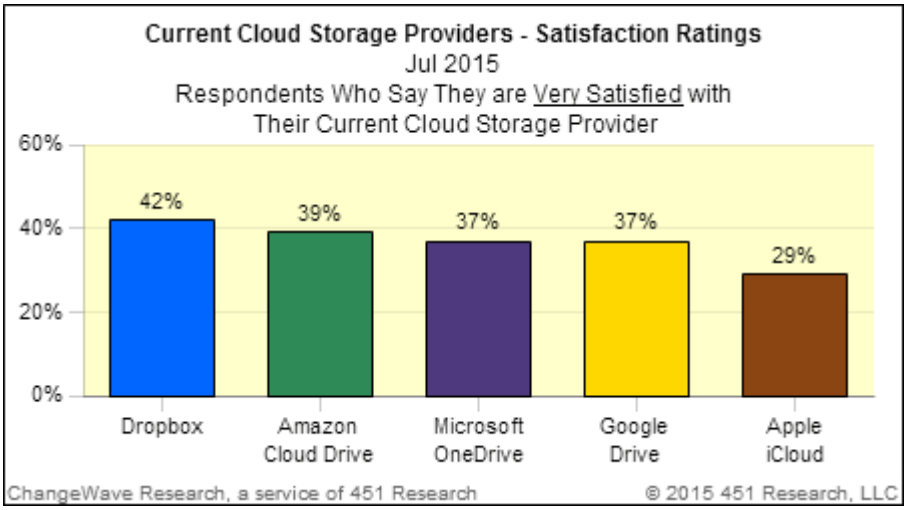
Two-in-five (40%) respondents say they now use a cloud-based storage service, although that's down 4-pts from the previous survey in January. Another 6% say they plan to begin using cloud storage services over the next six months – up 1-pt since January.

Among current and planned users of cloud-based storage services, Apple iCloud (50%; down 3-pts) remains the top choice.



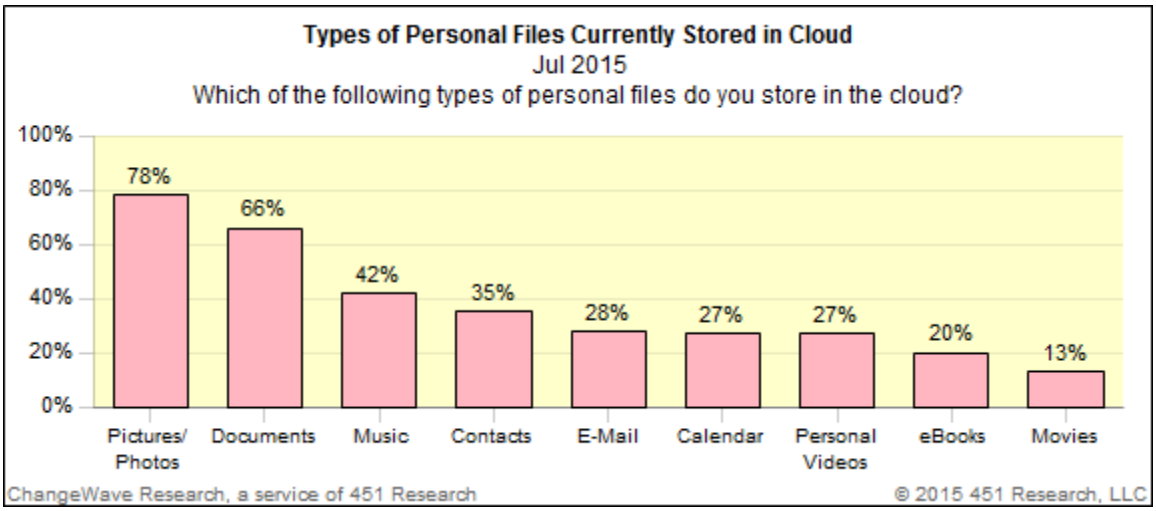
Dropbox (39%; down 4-pts) ranks second, followed by Google Drive (33%; down 2-pts) and Microsoft OneDrive (23%; down 1-pt). Fifth-ranked Amazon Cloud Drive (13%) is up 3-pts.

Customer Satisfaction. It's a tight field in terms of customer satisfaction, with Dropbox (42% *Very Satisfied*) edging out Amazon Cloud Drive (39% *Very Satisfied*) for the lead.



Microsoft OneDrive (37%) and Google Drive (37%) are tied for a close third, followed by Apple iCloud (29%).

Types of Personal Files Stored in the Cloud. *Pictures/Photos* (78%) and *Documents* (66%) are the most popular types of personal files consumers report storing in the cloud.



Consumer Perceptions of Cloud Security. The survey also asked all 2,012 respondents about their perception of cloud security, and 58% said they believe cloud storage services are secure (8%*Very Secure*; 50% *Somewhat Secure*) – up 4-pts since January.

Not surprisingly, current cloud users are much more at ease about security than non-users:

- Three-quarters (76%) of current cloud users believe cloud computing services are secure (15%*Very Secure*; 61% *Somewhat Secure*).

- Among non-users of cloud storage, 45% say they are secure (3% *Very Secure*; 42% *Somewhat Secure*).

III. Microsoft's Quest to Cut Carbon

Microsoft's quest to cut its carbon emissions dates back to 2012, when it announced plans to become carbon-neutral by FY 2013.

The decision to go carbon-neutral wasn't remarkable in itself. Other large tech companies had made similar commitments prior to the Redmond, Washington-based giant, and if anything, Microsoft was a latecomer (for example, Google claims to have been carbon-neutral since 2007).

But where Microsoft has led its competitors is in applying rigor to a claim that is often ill-defined and hard to assess (carbon neutrality can mean practically anything a vendor wants it to). It backed up the 2012 announcement by imposing an internal tax on carbon emissions – including a chargeback mechanism to collect the resulting carbon fees from individual departments.

Simply put, after identifying the departments creating the most CO_2 and providing incentives to curb emissions, the resulting carbon fees have been collected and allocated to support environmental initiatives across a range of business units – including datacenter operations.

Despite such a proactive stance, the company admits that carbon fees haven't had as much impact on its datacenter site selctions as the lure of network access. In other words, it still prioritizes other factors over access to renewable energy. Moreover, it has yet to disclose the size of its carbon-emissions fund.

Nonetheless, Microsoft is supporting a range of energy and datacenter projects via its carbon-chargeback mechanism – some which have the potential to be groundbreaking.

Datacenters, Energy and the Cloud

First, the company is investing in renewable energy via long-term power purchase agreements (PPA). Microsoft reports that PPAs are providing it access to low-carbon power in areas where it has datacenter infrastructure, while also enabling it to hedge future energy pricing.

In 2013, for example, Microsoft signed a 20-year PPA (with RES Americas) to purchase 100% of the energy from the Keechi Wind Project in Fort Worth, Texas. This 55-turbine wind farm is on the same electric grid that powers Microsoft's datacenter in San Antonio.

Funds from the carbon fee are also being used to explore the integration of fuel cells directly into datacenter racks. The pilot phase of a 2014 project was based on a hydrogen fuel cell, but the second phase will be based on a solid oxide fuel cell running on natural gas. While the testing has been done on single racks, it will eventually move to a multi-rack pilot – with the biggest challenge being cost-effectiveness at the multi-MW scale.

Employing yet another approach, Microsoft is running a pilot project to use biogas from a water-reclamation facility in Cheyenne, Wyoming, to power a small 200-server datacenter. The company claims the facility is the first zero-carbon datacenter (HP also says it has created a zero-carbon datacenter).

Importantly, the carbon fee addresses Microsoft's need to keep energy costs and carbon emissions under control while increasing its investments in cloud services and related datacenter infrastructure.

Along with fellow hyperscales Google, AWS, Dell and others, Microsoft has expanded its cloud datacenter capacity dramatically in recent years. So while the carbon fee is a cost for its lines of business, it's a tangible incentive for creating long-term efficiencies that will help Microsoft better compete with its rivals.

To date, the company says it has used the proceeds from its various departments to purchase more than 10 billion kilowatt-hours (kWh) of low-carbon power, and to reduce its carbon emissions by 7.5 million metric tons of carbon dioxide equivalent (mtCO2e).

IV. Health Info Sharing with IaaS: An Early Adopter Snapshot

Here's a close-up look at how a strong vendor-client partnership can lead to massive system-wide transformation.

UK-based Cambridge University Hospitals (CUH) is in the midst of a 10-year, £200m ($313m) shift from a fragmented, paper-based environment to one that accesses digital medical data via IaaS from an Epic electronic paper record (EPR) system.

The goal is for CUH to have a single patient information portal that is accessible anytime, anywhere and through any device – to save time, reduce the risk of human error and enable faster, more accurate decision-making.

The plan includes automated workflows to 'push' urgent results to clinical staff so they don't have to continually look for the results. In-line with this, nurses in CUH's operating theaters, post-op and intensive care are to work in a 'paper lite' environment.

HP is the main infrastructure-services partner for the project.

The IT Challenge

The transformation has required tackling CUH's legacy IT systems, some of which date back more than 10 years, and many – such as intensive care and the emergency department – that had no digital systems in place to manage patient care.

Cambridge University Hospitals also lacked Wi-Fi connectivity, and relied on an aging PC infrastructure that provided only limited remote access. Such old systems are inherently weak in terms of resilience and reliability.

After more than 1,000 clinicians reviewed eligible software modules and voted on their use, CUH shifted to the Epic electronic paper record (EPR) system. CUH used HP to provide workplace management and support services, as well as a network operations center to upgrade its IT systems software while also migrating legacy applications to the cloud.

Cut to the present – and now CUH staff have access to 6,000 new clinical desktops, 400 laptops, 500 handheld devices and 400 workstations on wheels to help deliver better patient care.

A 21,000-port HP network supports mobile working throughout the campus, while a bring-your-own-device capability for more than 3,700 users enables CUH's clinicians to securely access apps from their own devices, both within the hospital and externally.

When the system went live in October 2014, 150 people – including internal analysts and Epic and HP personnel – staffed an on-site command center.

Today, virtually everything is being done on the electronic system, and CUH has reached the point where change requests are all about adding to the system and expanding its capabilities.

Challenges and Obstacles

Such an ambitious organizational transformation meant that HP faced several challenges before the eHospital program could go live – everything from Wi-Fi installations to the scale of the training required to support this change.

Prior to launch, CUH wasn't sure which staff and associates the new system would touch, and, therefore, exactly who should be trained. Consequently, in a massive undertaking, 10,000 people were trained in nine weeks with the mantra that 'nobody is too important to train,' and everyone must have at least minimal training.

While every organization is unique, and CUH had many exclusive challenges to overcome, its journey from a paper-based environment to one that accesses all data via IaaS is a revelatory one that can be useful to other end users. It's a worthy example of how strong vendor-client partnerships can lead to successful system-wide change.

V. Hot Tickets

Do you have something interesting to share with the 451 Global Digital Infrastructure Alliance? Good, because we're looking for the ideas and observations on the minds of our members.

Simply send us an email and tell us what's on your mind. It's that easy!
451Alliance@451Research.com

All submissions play a role in our research program, and the ones that are ready for prime time will be highlighted in future editions of *Global Digital Infrastructure Trends.*

VI. Give Us Your Feedback

We want to hear your questions, suggestions and comments about the 451 Alliance. Simply send us an email at:

451Alliance@451Research.com.

We promise a quick reply.

~~~~~~

Managing Editor: Duncan Bowling

If you have any questions about your Global Digital Alliance membership, please contact Duncan.Bowling@451Research.com.

~~~~~~