

Average Inc.

...and how it can improve its use of information and communications technology (ICT)

Contacts:

Quocirca
+44 1753 754 838

Bob Tarzey
bob.tarzey@quocirca.com

Dennis Szubert
dennis.szubert@quocirca.com

Clive Longbottom
clive.longbottom@quocirca.com

Fran Howarth
fran.howarth@quocirca.com

Louella Fernandes
louella.fernandes@quocirca.com

Rob Bamforth
rob.bamforth@quocirca.com

The Average Inc. could do quite a lot to improve the ways it uses technology in order to reduce risk, ensuring business continuity, and to cut unnecessary cost. If Average Inc. needs to improve its use and management of its ICT infrastructure, then that means most real companies do as well.

- **Average Inc. has a single HQ with about nine branches. Its main IT resources are based in its data centre at the HQ.**
This is a business continuity problem waiting to happen. An outage of the HQ, for whatever reason, will leave most employees with nowhere to work and, even if they can set themselves up remotely, no IT to access.
- **The data centre has no backup power supply and a mix of underutilised servers.**
Much time is spent managing servers that are only used to about 15% of capacity. Average Inc. knows this and has started a virtualisation project, but it is early days.
- **There are servers in all its larger branches, which local staff with limited IT skill are expected to manage.**
Not only does this take up valuable time for branch-based staff, but there are often outages and backups are not guaranteed.
- **Across its locations, Average Inc. has a jumble of printers, scanners and faxes from many different manufactures.**
This is expensive to manage as there are no real economies of scale when it comes to buying consumables and employees waste lots of time fixing devices when they could be carrying out more productive tasks.
- **Average Inc. sees a lot of benefit in enabling its employees to work remotely but this is done in an ad hoc manner.**
There is little standardisation of the devices used, the way remote network access is procured and the security of access. There is much that Average Inc. could do to reduce cost and risk of remote access to IT for its employees.

BRIEFING NOTE:

This briefing has been written by Quocirca to address issues faced by companies with regard to ICT.

The report draws on Quocirca's knowledge of the technology and business issues faced by companies and is based on primary research carried out in this area.

As always, Quocirca is grateful to those who take part in such research without which these reports would not be possible.

Conclusion: Average Inc. is reliant on technology, but there is much it can do to ensure critical resources remain available at all times and are not a cost drain. Only when it gets these issues under control will it get full value from its technology investments.

Average Inc. (or Ltd, GmbH, BV, Pvt, SARL)



Of the six billion or so people on Earth there is probably no one that exactly matches Mr Average. However, it is still possible to gather the facts and describe what that single person might look like. The same is true of companies.

This report describes the average company and how it makes use of information and communications technology (ICT). It goes on to examine some of the risks companies face through bad practice and the remedial action they should take.

It turns out there is quite a lot Average Inc. can do to improve the way it uses technology. By definition, many companies will have worse practices than average. Quocirca hopes they will find the suggestions in this report useful.

Conversely, many others will, of course, be above average. Well done to them, but they need to guard against letting standards drop and losing the competitive advantage gained by good use of technology. This report provides a standard for comparison—defining the level that, in 2008 at least, they should endeavour to stay above.

Average Inc.'s ICT infrastructure

These figures are based on real world research that Quocirca has conducted in the last 12 months and are aggregated from a number of projects.

Average Inc. looks like this:

- ◆ 1,500 employees.
- ◆ A single main office (HQ) with nine branches—four large, and five small, all in the same country.
- ◆ 65% of its staff are IT users (just under 1,000).
- ◆ The four large branches each have an on-premise server running Windows Server 2003, which is used for email, file and print management.
- ◆ The smaller branches access central servers housed at HQ over broadband connections.
- ◆ They make use of a privately owned wide area network based on BT leased lines linking its HQ and four large branches.
 - The internet is relied on to connect the five small branches (“8 meg” ADSL with 10 or 20 to 1 contention).
 - There have been issues with network performance and caching software has been installed on branch office and data centre servers to try and improve this.
 - There is no data encryption for network traffic unless it is built into the application.
- ◆ Average Inc. has just started to open its supply chain management application to certain external

organisations using a web-enabled interface accessible over the internet, to allow:

- Suppliers to check inventory.
- Customers to check order status.
- ◆ PCs in all branches and HQ run a mix of Windows XP and older Microsoft operating systems.
- ◆ Most IT management is carried out remotely by third-party experts, but local branch office staff are relied on to do their own backups, which, as far as anyone knows, are done to tape and stored onsite at the branch. There is no checking the validity of backups or rehearsing for recovery.
- ◆ There is no standard for printers, scanners and fax machines and some of the branches and HQ departments have made their own purchases. This has led to a complex mix of products and software that is underutilised and incompatible with each other requiring different consumables.
- ◆ The company-wide telephone network is based on a traditional PBX system. However, Average Inc. has just started using VoIP to communicate between HQ and the larger branches and there is ad hoc use of other collaboration tools such as IM and web conferencing.
- ◆ A managed service is in place for spam filtering and there is anti-virus software on all desktops. However, there is no restriction on web access or use of USB devices, writable CDs/DVDs or other storage devices.
- ◆ Mobile IT is becoming important for Average Inc.—about 20% of its employees now access IT remotely:
 - 15% (including fields sales, management and some others) are issued with laptops.
 - Internet access in the field is via 3G data cards provided under corporate contract or ad hoc wireless access via commercial hotspots, which is expensed.
 - 10% use handheld devices (subset of the laptop users) that are used primarily for mobile email. There is a mix of BlackBerrys, Microsoft Windows Mobile phones and Symbian/Nokia smartphones, mostly company issued, but a few employees have been allowed to use their own devices.
 - 5% of employees are field service engineers who are supplied with Symbian-based smartphones to log faults and request spare parts. All are company owned.
 - Standard mobile phones are provided by the company to another 10% of employees where needed for business use. These are not

integrated into the corporate telephone network.

- A small number also expense use of private mobile phones.
- About 10% of employees are allowed to use their home broadband connection for business use and they expense the monthly fee. They are either using a company supplied laptop or a privately owned home PC.
- ◆ Management and hosting of Average Inc.'s public website is outsourced.
- ◆ Average Inc. has a single data centre as follows:
 - A converted room in their HQ.
 - No shortage of space.
 - 20 servers, at the last count.
 - Most servers run Microsoft Windows Server 2003 and .NET, but some of older servers are still running NT.
 - Email is run on some of the above servers using Microsoft Exchange.
 - Two servers running Red Hat Linux are used for Average Inc.'s intranet.
 - There is an old Sun Solaris server running some important business applications.
 - A virtualisation project was started a year ago using VMware and includes 25% of the Microsoft-based servers.
 - There have been no problems with power supply and there is no general purpose backup uninterrupted power supply (UPS), although some individual servers have this built in.
 - There are mumblings from Management about the amount of power used by the data centre, but power use is not billed or measured separately.
- ◆ IT is primarily managed in-house, with third-party consultants drafted in from a trusted partner when required.
- ◆ The board has said it wants to include an environment audit in the next annual report and that this should cover IT.

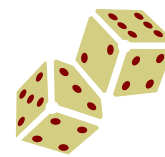
Areas for action: mitigate risk and reduce cost

There is no ideal ICT infrastructure as the requirements vary greatly from one company to the next but there is plenty Average Inc. can do to get its house in order. The primary areas of focus should be on reducing both risk and cost. Through doing this Average Inc. will find it easier to derive better value from its use of technology.

No company, including Average Inc., is likely to be able to afford to implement all these recommendations immediately, although this does provide a checklist for

any organisation to review its ICT infrastructure against and set objectives.

Areas of risk



- ◆ Average Inc. has a major business continuity problem. If its HQ is compromised in some way, the whole business will cease operating. This is because both the data centre and many of its employees are housed there. Even a power failure at HQ will take the whole business out, as there is no UPS. This need not be the case. If the data centre was located elsewhere, other branches and remote users could still operate even if HQ was compromised.
 - Mitigation: use a co-location provider for the data centre.
 - Good co-location providers will manage their use of power efficiently—it is in their own interest.
 - At the very least, if co-location is not accepted, backup power has to be provided.
- ◆ A subset of the above problem is that there is no redundancy (backup resource) in place for critical applications. Even if the data centre is outside the HQ, this would still be an issue. This is particularly critical now some applications are being opened up to external users, as an outage does not just affect internal users.
 - For critical applications, the co-location provider could also provide redundancy. However, when applications come up for renewal, considering software as a service (SaaS) offerings would also achieve the same objectives and are easy to share with external users.
- ◆ Network changes:
 - To maintain voice quality and other recommended UC (unified communications) services (see below), there is a need to get some guarantees around quality of service capability; switch to an MPLS network.
 - To ensure that all data is transferred in a secure manner, a virtual private network (VPN) should be put in place for all remote users and the smaller branch offices accessing the main network.
 - For home workers using their own PCs, or for certain external users, an SSL VPN appliance would ensure a separation of home/outside computing from internal applications.
 - Look at deploying a network security and acceleration appliance in each branch, and

- choose one that can benefit remote users as well, i.e. it supports PC clients.
- More secure network management could also help address the performance issues by filtering email content and controlling user activity of the internet.
 - There will also be possible problems with network outage, as a highly redundant network topology is not practical. Here, some appliances that can failover to a 3G/HSDPA card can provide continuous access, even if the WAN cable is compromised.
 - Such an appliance will also help cut problems with network contention where ADSL broadband is used.
- ◆ Giving employees unlimited access to the internet is a high risk strategy. All activity should be monitored and controlled.
 - Many providers of managed email security services are now providing the same for web access. See if the email filtering service can be extended and, if it cannot, switch to a provider that can supply both.
 - Some vendors of network acceleration appliances also include web filtering capabilities.
 - ◆ The security risks of networked printers also need to be considered through using secure printing solutions such as print authentication where print jobs are only released for authorised users.

Areas of excessive cost

- ◆ Maintaining and managing in-branch servers with no onsite skills is expensive, not just in terms of management costs, but also because they will almost certainly be under-utilised.
 - Recommendation: consolidate servers in the data centre where they can join the virtualisation regime. Network investments will make WAN access to branch servers practical (small branches are doing this anyway).
 - An additional benefit is that IT management can take over responsibility for backups of all servers and ensure backup media is stored off-site.
 - The 20 servers already in the data centre plus those bought in from the branches are almost certainly underutilised. Consolidate all servers into the new data centre, and virtualise as many as possible. This can cover both



- Windows Server 2003 and Linux-based applications
 - Moving away from NT would reduce management costs.
- ◆ In the above environment, the Solaris applications with their proprietary hardware are an anachronism. When practical, this should be reviewed so they can be run on the virtualised platform or be switched to a SaaS offering. However, if this is not practical, in the short term, these applications can still be moved to the co-location provider's facility and some virtualisation platforms will also support Solaris.
- ◆ Standardise PCs at the XP level to reduce management costs. There is no major benefit to be gained from moving to Vista at present.
- ◆ An unmanaged printing and imaging environment is a major cost, not just in terms of consumables but also of the time taken to fix devices. Obviously faxing, printing and scanning capabilities need to remain in branch offices, but companies can, over time, standardise on multi-function printing devices which can be managed remotely and which will allow for cheaper purchasing of consumables through economies of scale.
- ◆ Get rid of the PBX.
 - The company is already using a range of IP communications tools including VoIP and instant messaging. The recommended network investments would support more wide-ranging use of IP-based collaboration tools. A unified communications investment would standardise this, eliminate the PBX, and cut communications cost between branches and on long distance calls.
 - Mobile users do not need another fixed phone back in the office. Make their mobile phone their principal phone and consider pico-cells linked to the UC system for managing in-office mobile usage.
- ◆ Ad hoc expensing of wireless access in the field is expensive. Consider contracting to a supplier who will provide access to services from multiple vendors at home and overseas. 3G data cards and home broadband access should be brought under single contracts and rates negotiated based on enterprise usage patterns.

About Quocirca

Quocirca is a perceptual research and analysis company with a focus on the European market for ICT. Quocirca reports are freely available to everyone and may be requested via www.quocirca.com.