HOW
ENGINEERS
CAN USE
CLOUD COMPUTING
TO OPTIMISE THEIR
IT INFRASTRUCTURE

NATIONAL IT SOLUTIONS

We provide reliable IT consulting, support services and managed IT solutions. Our aim: Greater productivity and profitability for your business.

Index

NATIONAL IT SOLUTIONS

You Can't Move It All to the Cloud

When enterprise cloud computing first entered the scene, there was a huge rush to jump on to the bandwagon. Many companies, big and small, moved their technology requirements to the cloud without accurately assessing the correct option for their business.

A few years down the line, the drawbacks of hasty cloud adoption are being revealed as many businesses need to reconsider their cloud strategy .

Your business needs to know how to optimise cloud usage without having to bear any of the disadvantages associated with it. The comparison chart below covers some of the advantages and disadvantages of cloud computing and presents a listing of what should and shouldn't be moved to the cloud.

👍 Advantages

Cost: Investing in hardware and software for multiple users can burn a hole in the financial portfolio of most businesses. Cloud technology may significantly lower companies' IT expenses.

Unlimited Storage: Increasing storage on cloud is as easy as contacting your provider and asking for it. Traditionally, increasing storage capacity required the purchase of additional hardware that drove up costs and office space.

Anytime, Anywhere Access: Your employees can access any data they need from anywhere, since they are always connected to the organisation's core information centre via the cloud.

Quick Deployment: Installing and implementing a new software application is no longer an ordeal. Your cloud provider can get you going within minutes.

Ideal for the Cloud: Exchange, Email archiving, Backup, Spam protection, Web security.

👎 Disadvantages

Cost: Ironically, what is generally seen as an advantage, may also be the cloud's downfall. Several instances may lead to a sharp increase in your cloud computing costs, for example: attempting to customise it to your business' specific needs.

Security Concerns: It is believed that data in the cloud is more prone to hacks and malware attacks. Datacenter owners do take sufficient security measures, but concerns remain. Make sure you have full visibility of the security measures employed by your preferred cloud provider.

Privacy Laws: Some providers store your data in datacenters located in other countries, where privacy laws may not adhere to Australian Business standards. Opt for a provider that stores your data locally.

Latency Issues: Some files (especially larger ones) may display latency causing frustration and delays during potentially crucial business interactions.

Not so Ideal: File access, Printing, Windows Authentication and some Vendor-specific applications. (Note: Depending on the network infrastructure and internet bandwidth, these services may be moved to the cloud.)

NATIONAL IT SOLUTIONS

Email Archiving
-Not Another Hard Drive

Increasing email volumes, decreasing IT budgets and the rising number of legal discovery issues are driving email administrators to seek out ways to stay on top of it all and getting another hard drive or tape isn't one of them.

Traditionally, capital expenditure for email archiving and search solutions included:

- Expensive server platforms
- Costly storage management and search software
- Operational expenses (Managing, backup, upgrading servers etc.)
- Several gigabytes or terabytes of disk subsystems
- Additional data center costs

With most businesses now moving their email archiving to the cloud, the traditional costs have been drastically reduced.

Besides monetary savings, several other factors make a business case for archiving your engineering firm's emails in the cloud:

E-Discovery: Cloud providers have in-depth knowledge of e-discovery and can effectively manage your business' search and retention policies.

Regulatory Compliance: There are business regulations internationally that require protection and availability of information in electronic communications.

Storage and Access Limitations: Message archiving is a highly specialised function and calls for a centralised archival technology. This centralised solution tends to reduce per-user storage and hinders access control across the organisation.

Staff Efficiency and Green IT: Outsourcing to the cloud allows businesses to get more out of their existing IT with less staff. Besides, they can cut down on their hardware resource usage on-site, thus promoting green IT.

> " Enterprises continue to face challenges on email policy definition, ingestions of personal archive files, scalability and complex deployments. Cloud archiving solutions address a number of these challenges.
>
> **– Sheila Childs and Kenneth Chin,**
> *Analysts, Gartner*

Spam Protection
– Beyond Your Firewall

Spam. Most businesses believe it's just an annoyance that consumes time and bandwidth. On the contrary, several research results reveal that it is often the cause of data breaches, identity theft and potentially very high monetary losses.

Move Your Spam Protection to the Cloud

Move spam protection to the cloud, instead of relying on your firewall or on-site antivirus to take care of it. Why? Here's the answer to that $20.5 billion question:

1. Spam doesn't reach your server, thus reducing the size of your email database (consequently storage costs).

2. No local anti-spam software needed. Cloud service providers constantly update their spam protection algorithms, thus minimising the risk to your business.

3. Spam accounts for up to half of your email volume and you can imagine how much bandwidth these junk messages consume. Moving anti-spam to the cloud, therefore results in huge bandwidth savings.
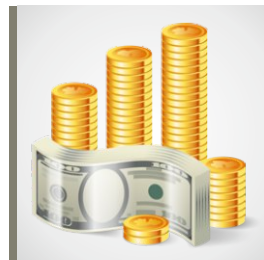
Spam costs businesses **$20.5 billion** annually in decreased productivity and technical expenses (Radicati Research Inc.)

Average annual loss per employee because of spam – approx **$1934** (Nucleus Research)

40% of UK SMBs have suffered a data breach directly because of spam (Opinion Matters Research)

> " Today's SMBs are four times more at risk of malware attacks than larger companies. Despite the risk, some just cross their fingers and wing it because buying, deploying and managing security systems is too complicated.

Tom Powledge,
VP, Symantec

NATIONAL IT SOLUTIONS

Backup
– Cloud Convenience

Alex Butera, *Director, National IT Solutions* discusses the reasons why a cloud backup strategy is *the* ideal solution to meet most business backup and disaster recovery needs.

Q. Why should engineering firms opt for cloud backup solutions, as opposed to conventional backup on-site?

Butera: I'll answer this question based on the specific backup strategies used:

Tape Backup: Tapes are cheap to purchase, but wear out over time. Also the backup process is manual and quite tedious.

Backup to disk drive: This backup option may be better than tape, depending on the type of backup strategy selected - file based or image based. Again, this option requires extensive user interaction .

These options are primitive. Cloud backup solutions, on the other hand, require zero user interaction and provide several other benefits including:

- Encrypted data protection to ensure your data is 100% secure
- Onsite backup for fast recovery
- Locally based off-site data centre for fast recovery in case of a disaster
- Backup file checks to ensure files are not corrupt and restorable
- Comprehensive reporting

I see this solution as a no-risk, peace-of-mind option for engineering firms. Everything is done automatically in the background with no interaction required from your employees. No need to worry if a disaster strikes or your server is stolen, you'll be back running your business within hours, not weeks.

Q. What are the disadvantages associated with cloud backup?

Butera: I doubt there are any perceptible disadvantages. Offsite backup may be slightly more expensive than conventional backup methods, but how do you put a cost on reliability and productivity?

Q. What is your advice to engineering firms that plan to move their backup to the cloud?

Butera: When moving your backup strategy to the cloud, we recommend you to get the following questions answered from the cloud provider you choose:

1. Where is the data centre located?

- For fast recovery in case of a disaster, make sure the data centre is located in the same city as your head office
- To adhere with industry compliance make sure the data is kept in Australian datacenters and not overseas.

2. How often do they check data for corruption and restorability?

- Make sure your backup status is monitored on a regular basis and frequent restore checks are completed

3. Do they offer a spare server in case of disaster?

- If your server was stolen or a disaster struck, how soon can you get a new or spare server?

Finally, make sure you choose a reputable IT provider that specialises in cloud backup solutions.

Web Security
– Stress Free Browsing

Lack of web security can cost your business thousands. Employees access the web daily and every time they use a web browser or connect to a web application they put your business at risk unless you use a robust web security system to combat hackers, phishers and malware. See the statistics below to gauge the importance of strong web security measures at the enterprise level.

Move Web Security to the Cloud

Most installed internet security programs don't offer sufficient defence against the range of vulnerabilities and security compromises your business faces on a day to day basis. Our web security cloud application offers business grade web filtering as used by many corporate companies at an affordable price for Small to medium business.

An IDC report explains their importance very powerfully: "Market demands for Web Security solutions have changed and must address a much broader set of functions. Explosive growth of Web-based technologies in the enterprise (i.e., social media, mobile apps, software-as-a-service/cloud infrastructure) and the bring-your-own-device (BYOD) phenomenon are forcing rapid change on the Web security market."

This excerpt from the IDC report clearly articulates how ineffectual conventional web security softwares are.

Are you ready to make the move?

73% of organizations have been hacked at least once in the past two years through insecure Web Applications   (State of Web Application Security Survey, Ponemon Institute).

13 – The average number of "serious" vulnerabilities on any website (WhiteHat Security)

US users land on malicious websites about **285 million** times per month by clicking on results from the five major search engines (McAfee Inc.).

20% of consumers terminated their relationship with a company after being notified of a security breach (Ponemon Institute).

"There is a common misconception that emails constitute the biggest security threat from the Internet. But our survey shows that up to 30 percent of companies with 500 or more staff have been infected as a result of Internet surfing, while only 20–25 percent of the same companies experienced viruses and worms from emails.

Per Andersen,
Managing Director, IDC Denmark

NATIONAL IT SOLUTIONS

Aware 360°
– Keep Your Secrets

Most data thefts, viruses, malware and spyware attacks to your company are caused intentionally or unintentionally by your employees.

Inappropriate communications, the loss of confidential data and intellectual property can cost your organisation millions in legal fees, revenue and market standing.

Former Intel Employee Pleads Guilty to Data Theft

April 9, 2012 – Bloomberg:

36-year old Biswamohan Pani has pleaded guilty of stealing chip design documents valued at several hundred million dollars from his former employer, Intel.

The engineer quit his job at Intel on June 11, 2008, and joined AMD on June 2, while he was still able to access Intel's servers. Pani downloaded "numerous" confidential documents that were originally estimated to be worth about $1 billion, but were tagged by Intel with a value of about $200 to $400 million later on. The engineer apparently intended to advance his career by bringing the documents to AMD.

Move to Aware 360°

Aware 360° records all activity on any computer within your organisation and allows you to view email correspondence, instant messaging, internet activity, database queries and documents accessed or changed on that computer.

The Aware 360° online console can be reviewed and managed by authorised personnel only. Many organizations that have implemented this application report a marked increase in employee productivity.

Plan Your Move
TODAY

Your business deserves more than a blind leap of faith to the cloud.

Strategy, insight and extensive analysis will help you chart the right course towards moving the "right" components of your business to the cloud.

Is your business making optimal use of cloud computing?

Get your needs assessed and a comprehensive cloud computing strategy created by an expert.

**Get Your Free
Cloud Computing Audit
TODAY**

Contact Us

Founded in 2002, National IT Solutions is a fully owned and operated Australian IT Consultancy Company specialising in Information Systems. Our extensive experience in the Small to Medium Business (SMB) segment enables us to provide managed IT solutions and integration advice to many corporate clients by offering comprehensive information for building cost effective, stable and cohesive IT systems.

National IT Solutions provides a range of technology solutions, to holistically strengthen your business. These include:

- **IT Support**

- **IT Consulting**

- **Managed IT Services**

- **Cloud Services**

- **Business Continuity Planning**

- **Virtualisation**

- **Security Services**

- **Email / Spam Protection**

To learn more about our company and what we can do for your engineering business, contact us today.

National IT Solutions Pty Ltd.
114 \ 566 St Kilda Rd,
Melbourne,
VIC 3004

Call Us (Toll Free): 1300 – 795 – 395

Call Us: 03-9533-9888

Email: info@itsolutions.com.au