



Cloud security and your business



As technology improves, the world is becoming more connected. The internet features in all aspects of our life, from our social media accounts, to our businesses, even to finding a recipe to cook for dinner. With this shift, more and more businesses are turning to the cloud in order to store their data. So what is the cloud? And how can you use it to make your business's data safer and more user-friendly?

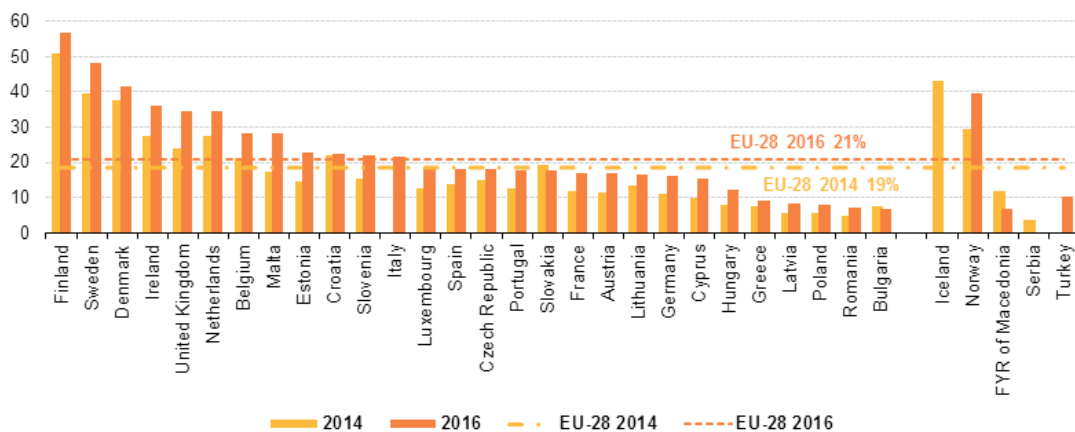
The cloud

A recent survey of 1,060 IT professionals found 95% were using some kind of cloud software. While the cloud is becoming more prominent, it's still a relatively new way of running programs and storing data. In the last ten years, software has moved from user-installed, to cloud based, where applications run off the Internet from servers off-site.

While Australians are far from best in the world for Internet speed – now ranked 50th in the world at an average of 9.6Mbps, it's a far stretch from the 1Mbps speed enjoyed by Internet users 10 years ago in 2007.

With this faster Internet, companies have the opportunity to store their data on the cloud, running their applications and storing data on servers possibly thousands of kilometres from where they're working. Statistics from IBM estimate that in the last two years, 90% of all digital data was created.

Businesses are moving to their data and programs to the cloud at increasing speed. Software as a service is becoming common, with companies automating processes like HR in the cloud. In Europe, the percentage of enterprises using the cloud went up from 19% to 21% between 2014 and 2016, and the growth is continuing.



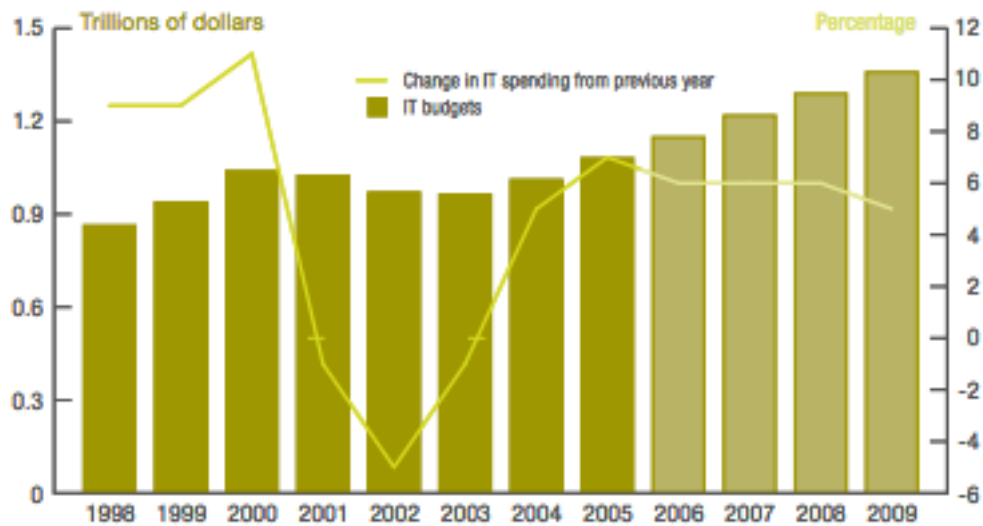
Italy: break in series; Iceland, Serbia: 2016 not available; Turkey: 2014 not available

What are the benefits of making the move? And how can you protect your data if you do so?

Benefits of moving to the cloud

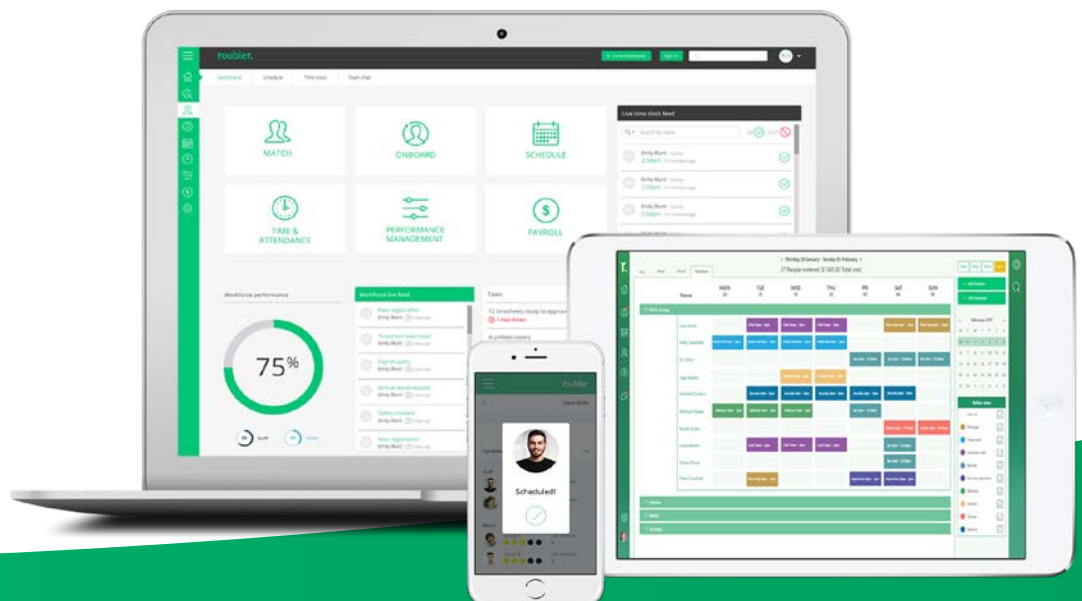
Better IT support for a fraction of the cost:

While this may sound like some kind of marketing gimmick, in most cases with cloud applications, it could not be more true. With any program there are always updates, patches, and backups needed to keep it working optimally. Cloud applications remove the need to install and update these issues yourself. What's more, the cloud application company does most of what an experienced IT professional would do, without you having to pay for IT in-house. With IT budget growth rates decreasing, this could help decrease the strain on your IT department.



Source: IDC, 2006

Although IT budgets have recovered somewhat from the 2000–2002 recession, they are experiencing declining growth rates each year and significant portions are being diverted to new compliance and security mandates.



Quicker updates

With normal business applications, you can potentially wait a year for the latest version. With a monthly subscription, not only do you have the benefit of using the latest software, but you no longer have to pay out one bulk sum for something that will be out of date within the year.

Accessibility

Cloud applications don't require a CD-ROMs or installed program on your computer. All you need to access your work is an Internet connection. Cloud companies are beginning to recognise your need to work from anywhere however you can, and are making the software available on nearly all possible devices.

Continuity

Bad things happen at the worst times. A leak in the roof could damage your equipment, someone could steal your computers, even a meteorite could destroy the very place where you work. The best part about cloud data is that it can be recovered quickly and painlessly, within hours, as it isn't stored on-site. The last thing you want when disaster hits is worrying whether you can save your work from the rubble.

Integration

Data from skyhigh found of the users of their platform, the average employee of an organisation uses 28 cloud apps. Cloud systems give you the ability to integrate software, seamlessly sending data from, for example, HR to payroll, or accounting to stocktake software. This way, information is quicker to access and doesn't get lost in the system. This makes your employees lives easier, keeping them engaged and interested.



Where and how is your data looked after?

When so much sensitive data is being uploaded and sent, it's important to know that your data is protected.

For most companies using the cloud, your data is stored on servers in what could be called "server farms" – massive warehouses of servers, run by managers and protected by security 24 hours a day. For professional cloud businesses, the journey between your device and the cloud server is secure; the data is encrypted before being sent or received, so no one can listen in to your data without your permission.

With all the precautions, data can still be hacked. So how do you prevent this from happening to your business? More often than not, it's not the safety of the cloud application that causes the issue. Rather, it is how you and your employees use it.

Ensure your passwords are secure and protected

When choosing a password, many people aren't the most creative or wide-reaching. People will often use the name of a favourite pet, birthday, or mother's maiden name, all of which are easily discovered. Combinations of these may seem complicated, but are in fact very simple to crack. It's a process of creating a password long enough that it's difficult to crack by brute force, but short enough that it can still be remembered. Correct Horse Battery Staple and other similar sites help you generate a random password to protect your data.

Make sure your passwords are different for every application, and not related to you in any way. For even stronger protection, try passphrases. These are a little longer, between 20 and 30 characters.

Multi-factor authentication

For more security, some cloud apps supply another level of protection after your username and password. Also known as two-factor authentication, two-step authentication or two-step authentication, cloud applications can ask for another layer of identification, for example a code sent to another device, a fingerprint, or voice. This way, even if your password is discovered, your account remains safe.

Use the safety features included in your package

It's easy once you've set up your cloud application to ignore extra security information provided, but it could be the difference between safe and compromised data. For example, services sometimes provide information about times and dates of the last login, and where the account was accessed.

Make the most of anti-virus software

Malicious software, or malware, usually accesses your laptop when you click on a link or attachment from an unknown source. The first thing you can do to stop malware from accessing your data and stealing it from inside your computer is not click on any links or attachments you don't recognise. If this happens however, anti-virus software from a well-known and trustworthy company is incredibly important to have on your computer. Check it's legitimate with [virustotal.com](https://www.virustotal.com), and ensure it remains updated. Considering how easy it is to accidentally click on an unfriendly link, this is one of the most important ways of keeping your data safe.

Keep abreast of hacking or phishing techniques

Every day hacks and scams think of new ways to access your data. If you and your employees know the latest ways you could be coerced into giving away your password, it's less likely that the information will be compromised. Make sure employees know what kind of emails they will be receiving from you, so they don't fall victim to giving away their information to an email that seems professional, or a phone call from what sounds like a reputable source.

Most of the time, hacks to cloud security could just as easily happen to your data stored on your own computer. It's a matter of increasing security at your end, so the cloud companies have the most to work with when keeping your data secured. Make sure your employees are well versed in potential hacks, data security and storage. Employees should have the training to know what to do even if you're not around. Have them create strong passwords, include multiple layers of identification, and make the most of everything included in your subscription. Nothing is certain, but by reducing human error, and making small changes, you can make the most of this new technological age of cloud applications with the knowledge that your data is well protected.

References

eurostat,. (2017). File:V1 Use of cloud computing services, 2014 and 2016 (% of enterprises).png. Retrieved from [http://ec.europa.eu/eurostat/statistics-explained/index.php/File:V1_Use_of_cloud_computing_services,_2014_and_2016_\(%25_of_enterprises\).png](http://ec.europa.eu/eurostat/statistics-explained/index.php/File:V1_Use_of_cloud_computing_services,_2014_and_2016_(%25_of_enterprises).png)

Foth, M. (2009). Handbook of research on urban informatics (1st ed., p. 313). Hershey, Pa.: Information Science Reference.

Intro to Cloud Security | Small Business Guide | Xero. (2017). Xero. Retrieved 21 March 2017, from <https://www.xero.com/au/small-business-guides/business-management/cloud-security/>

Jager, C. (2017). It's Official: Australian Internet Speeds Are Still Terrible Read more at <https://www.lifehacker.com.au/2017/01/its-official-australian-internet-speeds-are-terrible-infographic/#8F3gl5B39GLXQmad.99>. Life Hacker. Retrieved from <https://www.lifehacker.com.au/2017/01/its-official-australian-internet-speeds-are-terrible-infographic/>

Kohgadai, A. 9 Stats on Sensitive Data Stored and Shared in the Cloud. Skyhigh. Retrieved 21 March 2017, from <https://www.skyhighnetworks.com/cloud-security-blog/9-stats-it-should-know-on-sensitive-data-stored-and-shared-in-the-cloud/>

PWC,. (2017). https://www.pwc.com/us/en/technology-innovation-center/assets/softwarepricing_x.pdf. Retrieved from https://www.pwc.com/us/en/technology-innovation-center/assets/softwarepricing_x.pdf

Vasconcelos, P. (2013). Where On Earth Is Cloud Data Actually Stored?. KrollOntrack. Retrieved from <http://blog.krollontrack.co.uk/top-tips/where-on-earth-is-cloud-data-actually-stored/>

Weins, K. (2016). Cloud Computing Trends: 2016 State of the Cloud Survey. Cloud Management Blog. Retrieved from <http://www.rightscale.com/blog/cloud-industry-insights/cloud-computing-trends-2016-state-cloud-survey>



www.roubler.com