White Paper: Information Security in the Cloud

Managing risks when you outsource all your data

Introduction

As we become accustomed to our data living "out there" in the ether rather than on our hard drives, disks or servers, we also accept the fact that our data sits in the hands of someone else far, far away.

If you are a charity, the donation scheme that Microsoft offers, giving away Office 365 for free, is so compelling that Chief Execs could feel compelled to make cloud fit their organisation no matter what the data security risks, because of all the other benefits it brings.

So what *can* you do to ensure you are responsible with your IT security when you don't control the infrastructure is lies within? The answer is quite a lot. This White Paper explains some of steps you can take, as well as the considerations and risks associated with storing your company files with a cloud service like Microsoft Office 365.

Considerations

As Gartner puts it: ""*Each cloud model requires a separate strategy. Whether you embrace it or not, you need to understand the reality and be aware of shadow IT. Security, whether you like it or not, must cater to the cloud security problem*," and in this "Internet of Things" age, there is of course no single solution to cover all your bases; you need a mix.

To make things more manageable, we can break down the IT estate into five core areas, and then look at implementing a strategy or policy for each:

1. **Data Retention**

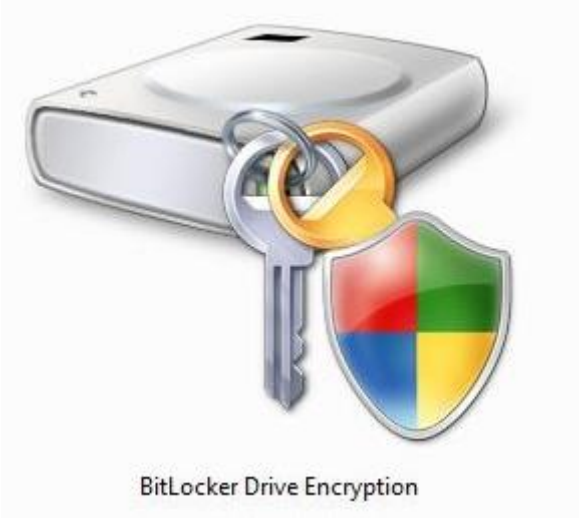
Many companies are required by law to retain old data for a certain period after use, often five or more years. Cloud systems often have presets which will delete old files forever when a user leaves, for example. This policy should be checked and adjusted to ensure you are compliant - Office 365 retention period of 30 days by default, and increasing this limit comes at a cost, so this should be checked and reviewed as part of a security review.

2. **Encryption**

One of the biggest threats IT security is accidental loss of devices like laptops. Applying whole disk encryption secures your devices in addition to the usual username and password needed to log into Windows. Furthermore, it encrypts all data on the disks, meaning even if you break open the laptop and connect to the disks directly, the data on there is useless.

The main consideration here is change management; implementing this on your devices will require our staff to enter two sets of credentials – usually a numerical pin code first, then their usual username and password. People will adapt to this, and it adds a significant layer of protection to your network, but change must be handled carefully with training and support given.

Windows 7, 8 and 10 comes pre-bundled with BitLocker whole disk encryption and is the easiest and most cost effective way to implement this for charities; we can provide case studies on its implementation for some of our clients if you are interested.



3. Liability

The Office 365 T&C's state their limit of liability is $5,000 or your last 12 months subscription fees should anything happen to your data. In reality, proving that any data loss was Microsoft's fault is going to be very hard and extremely expensive. With that in mind, including data loss cover in your liability insurance will help build up your risk resilience should your organization loose sensitive data.

4. Location – where is my data kept?

Many companies are required by law to provide evidence of where their data is stored – especially if you hold personal data such as names and addresses. Providing this information to auditors can be tricky if Microsoft holds all your data across multiple servers worldwide.

Recently the Safe Harbour Agreement – an attempt by the cloud providers to reassure Europe that their data is handled in accordance with local law – was deemed unsatisfactory by the European Court, and an attempt has been made to replace it with the Privacy Shield as a means to satisfy European regulators that US based cloud firms like Microsoft and Amazon will protect our data. However, these initiatives have not been ratified by the European Commission and have recently come under fire. How the UK will now handle their data protection laws outside of the EU will be an interesting development, but it's a fairly safe bet that we will retain existing restrictions on data movement after we leave.

Physical storage of your cloud data has been a grey area for many years now, and remains so. The sheer size of cloud providers' networks mean it's impossible for them to guarantee 99.97% service levels AND keep all your data in one place, in your own country, AND keep costs as low as they are.

Ultimately, if you need to store customer or donor or members' personal information, the advice is not to put these on public cloud providers like Office 365. Instead, consider using a hybrid approach – a private cloud / hosting setup such as Ethical IT's own bespoke cloud platform for sensitive data that stays in UK data centres, perhaps in conjunction with a cost effective public cloud service like Office 365 for your day to day email and shared file systems.

Data Protection Act 1998

5. **IT security best practice – mobile and desktop devices**

Agreeing, implementing and reviewing IT Security policies sounds onerous, but it really needn't be. Here's our Top 10 Checklist of items that you could include on a simple IT Governance document, that would cover off a large majority of risks and satisfy auditors that you are taking responsibility for your day to day security

1. **Complex Passwords are enforced, and rotated every 45 days**
2. **User Accounts are audited every month and old users deleted**
3. **Shared Drive permissions are audited at least once a year and permissions revoked for all but the essential staff on sensitive folders**
4. **Mobile devices have enforced 6-digit PIN lock protection enabled**
5. **Drive encryption is installed on all laptops; this can be BitLocker in Windows 7-10**
6. **Anti-Virus is deployed on all machines and compliance checked every 6 months**
7. **No staff have administrative permission over their own computer**
8. **USB drives are locked down to only accept encrypted drives secured with PIN**
9. **IT and Support staff have named admin accounts to ensure an audit trail**
10. **Complete backups are taken daily to a separate location, even on cloud storage**

Conclusions

Migrating to a cloud system such as Office 365 has huge benefits to most small businesses and is something we strongly advocate. However, this process can often leave a company with little power over their data day to day – something that is often overlooked.

In itself this is not a big issue; however your company is still responsible for its data. Proving to your customers or auditors or lawyers that you are in control of your data can be hard when using a cloud solution and may put your company in an awkward spot.

By following the above steps and best practice, you can be confident that you are being responsible with your data security policies and practices and minimising your exposure to risk.

Further Reading

ISO27001 is the international set of standards covering IT Security. Ethical IT achieved this certification in 2015 and we would be happy to help advise and support your organisation through this certification; please contact enquiries@ethicalit.net for further information