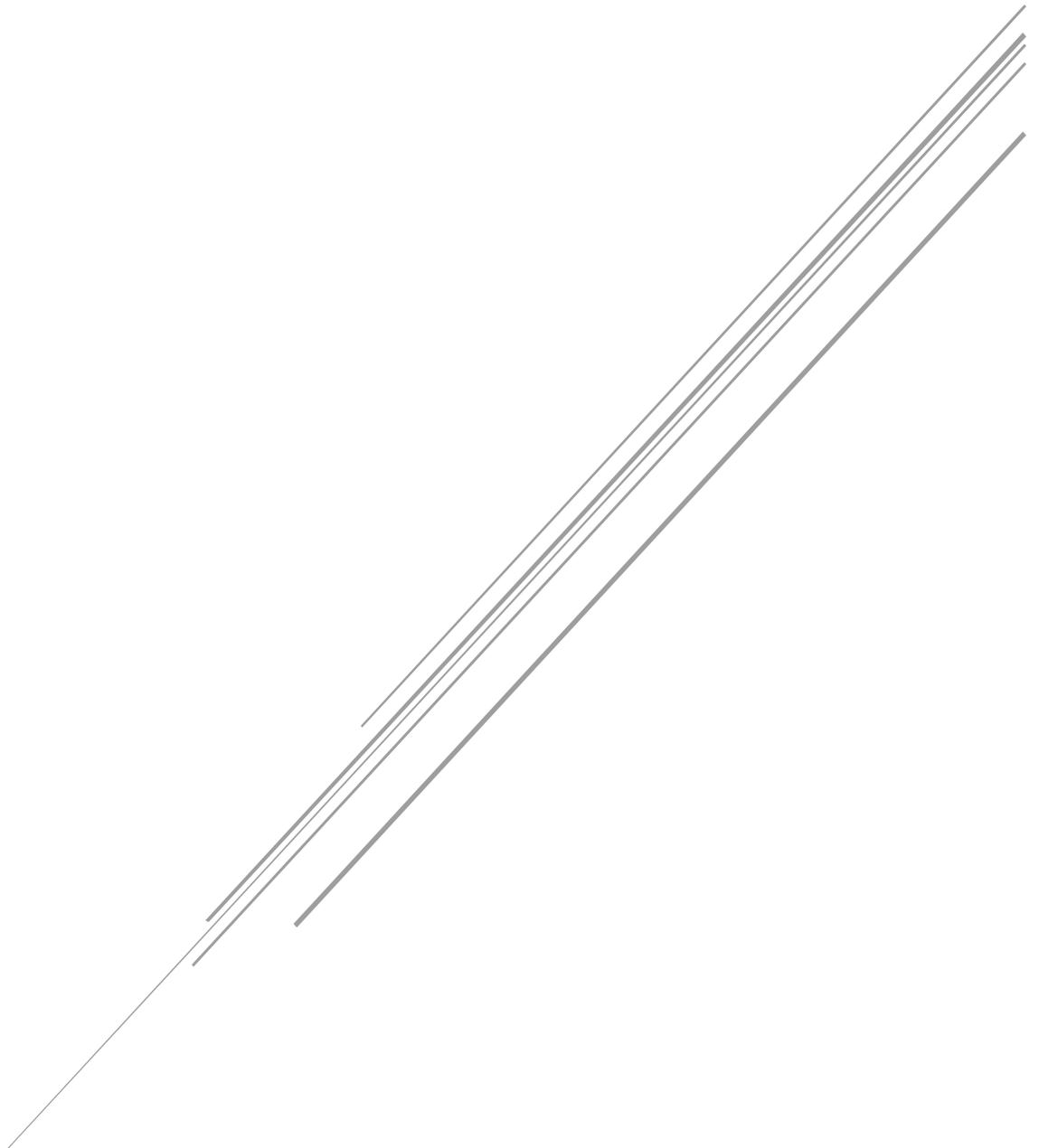


ENCRYPTION: IT REALLY IS YOUR RESPONSIBILITY

Encryption is important, don't leave it to others.



Taz Wake
Halkyn Consulting
Security and Risk Management Specialists

Encryption – it is your responsibility

Encryption is important, don't leave it to others.

Encryption is important. This has always been well known, and with the recent revelations about PRISM and related Government monitoring of communications, people have become understandably more interested in the topic. However, keep in mind the fact that doing encryption wrong is worse than not doing it. In recent years it has become more and more common for people to store personal data and commercial data on a variety of 3rd party platforms – Google Docs, Skydrive, Dropbox and Box etc.

Encryption needs to be locally managed

At the most basic level, if you host your data somewhere outside your control – be that a cloud provider or more traditional hosting session – then you really should be encrypting it. When you do use encryption it is of the utmost importance that you manage the keys yourself. Anything else is giving you a very dangerous false sense of security and means your encryption can be trivially bypassed without you even knowing.

However, this fundamental principle seems to have been overlooked with Google's latest PR campaign which looks to allay customer fears by implementing automatic encryption to all uploads. **This is a very bad idea.**

The Telegraph reported the news of Google automatic encryption¹ with the following:

"We know that security is important to you and your customers. Our goal is to make securing your data as painless as possible," Google product manager Dave Barth said in a blog post introducing the update.

Now, it is true that implementing encryption can be difficult, but that is largely down to the level of experience and expertise your staff have. **If security is important, then you absolutely must make sure you have the right people to do it.** If security is important, then this is really not the place to cut costs.

The article continues with this, also from Dave Barth:

¹ <http://www.telegraph.co.uk/technology/google/10254223/Google-boosts-cloud-security-with-automatic-encryption.html>

“If you require encryption for your data, this functionality frees you from the hassle and risk of managing your own encryption and decryption keys. We manage the cryptographic keys on your behalf using the same hardened key management systems that Google uses for our own encrypted data, including strict key access controls and auditing.”

Now this is a bit calculating and presents an image which isn't really true.

Remember the fundamental principle – if you don't manage your own encryption keys, your data is insecure? Well it applies here. It especially applies here.

Managing your own encryption keys may be a hassle, but it is less of a risk than trusting a third party to do it for you – especially a third party which has no real obligation to your stakeholders, is big enough to likely shrug off any legal efforts you make, refuses to acknowledge the jurisdiction of the ICO / Data Protection Act and was reportedly complicit in revealing data to the Government agencies it is implying it will protect your data from. If you rely on Google's (or anyone) automatic encryption then you are relying on them making sure all their employees are honest and legitimate, making sure that they never go out of business, making sure that they never engage in covert arrangements with Government agencies or other companies, making sure they never get hacked, making sure they never have an outage when you need access etc.

You may be confident that one or two of the above will never happen to your provider, but you actually need to be 100% confident that nothing bad will happen. Ever.

Isn't that asking a bit much?

Using automatic encryption may remove some hassle, but it significantly increases the risks your data faces, often to the point at which you are better leaving it unencrypted and assuming it has been compromised.

Encryption – the basic rules

When it comes to your encryption, there are actually some simple rules to keep in mind and the whole thing is easier than it looks. With encryption, the only hard parts are working out what technology to use and picking a suitable key (e. g. password).

1. **All your data must be encrypted locally.** Even if your provider uses SSL, before you send anything out of your immediate control you absolutely need to know that it is encrypted to whatever standard you have decided upon.
2. **You must manage encryption keys yourself.** These are the crown jewels and if you lose them or compromise them, your data is lost or compromised. However,

keep in mind, things that are important to you might not be as important to other people so you are the best person to look after your encryption keys.

3. **Store encryption keys separately from the data.** If someone has your data and your key, the encryption is meaningless. Keep them apart unless you need to decrypt / encrypt.
4. **Guard your encryption keys.** It should go without saying that your encryption keys need to be backed up and protected. If you have an information classification scheme, your encryption keys should be treated the same as the information they protect. Try to avoid falling into the trap of encrypting your encryption keys though... that just gets confusing.

If you live in a country where the state can force you to reveal keys (such as the United Kingdom, China etc.) or there is a risk someone could place you under duress, then consider a deniable container. This is offered by products such as Truecrypt² and gives you the ability to surrender the outer encrypted data while keeping your secrets safe. This is especially useful if you or your employees travel and there is a risk of unwanted attention as it means they can comply with any demands (lawful or otherwise).

The bottom line is that encryption is not hard, it is not hassle and if you really do think security is important you should be doing it. The key phrase, however, is that **you** should be doing it, not someone else.

Anything else means you don't really think security is important.

² Truecrypt is available as a free download at: <http://www.truecrypt.org/>

About Halkyn Consulting

Halkyn Consulting Ltd is a specialist security consultancy based in North Wales, experienced in providing security advice to local, national and international clients including government agencies, multinational corporations, small businesses and homeowners.

For more advice on how to properly use passwords or any other questions you may have related to security and protecting your home, business or other assets, you can reach Halkyn Consulting:

on the web at www.halkynconsulting.co.uk

by email to info@halkynconsulting.co.uk

or you can call us on +44 1522 940 858

