Document disposal - Don't take risks

Protecting the data that you throw away

T Wake
Halkyn Consulting
Security & Risk Management Specialists

Document disposal – don't take risks

There was a lot of press coverage of an incident where a cabinet office minister (Oliver Letwin) was observed throwing official documents into a public waste bin. It was reported that these documents contained a mix of information relating to counter-terrorism and correspondence from his constituency members.

The Guardian newspaper reported

> On Friday morning, the office of the information commissioner said it was launching an investigation into potential breaches of the Data Protection Act.
>
> The Daily Mirror reported that Letwin was seen on five separate days binning sensitive correspondence on terrorism and national security as well as constituents' private details in the park near No 10.
>
> In all, the Mirror claimed that Letwin threw away more than 100 papers containing private information, including five intelligence and security committee (ISC) letters. In one, MP Andrew Tyrie reportedly tells the ISC chairman, Sir Malcolm Rifkind, the committee "failed to get to the truth on UK involvement in rendition".
>
> Another discarded document referred to al-Qaida links to Pakistan, the newspaper claimed.

According to a statement from the Cabinet Office, the documents **did not** contain classified Government information and that "*most of the business Mr Letwin does in the park is constituency based*." However, there is now an investigation into the incident, so hopefully more details about what has happened here will become available in time.

While it can be seen as entertaining when a Government minister acts in this manner (especially as the Cabinet Office is responsible for directing the national security strategy), there are still some very important lessons that every organisation can learn from this.

First and foremost: **You absolutely must** ensure your staff are properly educated about the information they have access to and what is an appropriate and acceptable mechanism to dispose of it. If your organisation comes under heavy public scrutiny, or you handle a lot

personal data, then it is doubly important that you ensure all your staff are aware of how their actions may be perceived.

This leads on to the need to ensure that your policies and procedures for disposal of official (sensitive or otherwise) material **make sense** and are **easy to follow**. If they don't make sense your staff will ignore them. If they are difficult to follow, your staff will bypass them. There is no point getting frustrated or angry with your workforce because of this – just improve the security instructions.

On a related note – despite the mild furore around this current incident, it is possible that Oliver Letwin actually thought he was following procedures. Government security standards are driven by the Security Policy Framework (available for public download on the Cabinet Office website) which discussed disposal in Mandatory Requirement 45[1] but this is simply an instruction to use HMG Information Assurance Standard No 5. Interestingly the scope of this standard is magnetic disks and tapes, optical disks and solid-state devices. Better advice is available within the classified guidance provided by the Government Protective Marking scheme. On the whole this simply says that for low-sensitivity documents you need to "dispose of with care or destroy to make reconstitution unlikely."

In the case of Mr Letwin, I think it would hinge on your belief about what makes reconstitution unlikely. If you are a normal member of the public, it is certainly unlikely that someone will root through a public waste bin to reconstruct your paper work, but we really can't say the same about Ministers.

From this, we get the final "top tip" from the news today. **Properly identify and assess the threats you are facing and the importance of the assets you are protecting**. This should inform every stage of your security and risk management cycle. It should be part of the awareness training your give your staff and it should be the driver behind your choice of security controls.

[1] This article was originally written in October 2011. Since then, the UK Government Cabinet Office has revised and updated the Security Policy Framework so that technical Data Disposal is contained within Mandatory Requirement 9 and obliquely covered by Mandatory Requirements 6, 7 and 10. Unfortunately this has done a lot to muddy the water around what is permitted and what isn't with regards to disposal of paper-based data.

If you don't do this, you can almost guarantee that your security controls will either fail quite dramatically (and why is an MP doing constituency work in the park anyway – what is wrong with his office?) or you will fail to take advantage of opportunity because your controls are too restrictive and prevent your workforce from maximising their potential.

These three simple security steps are so important; it won't hurt to repeat them:

1. Educate your staff about security and their role in it.
2. Have good, sensible and practical security policies, procedures and standards.
3. Carry out diligent and directed threat based risk management.

If it helps, print them out and plaster them over every surface you can see. Repeat them until they have invaded your dreams. When everyone in your organisation is doing this, you will have optimised your security posture.

These three simple steps can take your organisation 80% of the way towards having robust security and, better still, a strong culture of security that allows you to exploit new areas without harm. Ignore them at your own peril.

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 at www.halkynconsulting.co.uk or info@halkynconsulting.co.uk