Data Protection in the UK Public Sector

The changing face of data security

By Barbara Hudson, Product Marketing Manager, Sophos and Tim Holmes, Sales & Marketing Director, Sustainable Gov

Recent news of major data breaches may make good headlines for the press but essentially they have highlighted the need for a re-think of data security in the public sector. In this whitepaper, we look at how the public sector in the UK is shaping up based upon a recent survey, and give some simple steps to improving data security.
Data Protection in the UK Public Sector The Changing Face of Data Security

Data, data everywhere

The way we work is changing. Mobile computing and fast wireless connections provide the infrastructure to exchange, access and store data from any location. But with this change there are also increased risks. Data is one of this century’s most precious commodities – allowing it to be lost, stolen or corrupted could have dire consequences.

These challenges are felt even more keenly in the public sector, which handles inordinately large amounts of data and has the entire public pressing for its protection. The risks are inherent not only from a financial perspective – Government data could have implications for even the most serious matters of national security, making it paramount that the correct safeguards are in place.

The public’s perception of public sector data handling is often poor, fuelled by stories in the media of embarrassing breaches and losses by civil servants. Repairing this reputation has long been a source of strife for policy makers, a task that will necessitate improved systems and processes to be put in place before public relations victories can follow.

In this whitepaper, we will take a look at how public sector organisations in the UK deal with data security today with a particular focus on mobile device security. We will also highlight areas which could be addressed, both by the organisations themselves and by the ICO (Information Commissioner’s Office), which would greatly improve the security of data in the public sector.

What has changed?

Analysts have been talking about the ‘consumerisation of IT’ for a number of years but only now is it really turning into a reality. This phrase refers to the ever finer line between the business and personal use of a device and smartphones are a prime example.

When you tolerate the private use of a device, be it a smartphone, laptop or tablet, it is generally because it has a pleasant side effect, namely that your employee will also perform work-related tasks outside of office hours – such as checking work emails. If you also allow your employees to bring their own mobile devices to work and use them there, this is taken to the next level. This method is known as Bring Your Own Device or BYOD. What at first sight may seem like an extremely attractive money-saving measure – one less investment to make from a tight budget – is actually both a challenge and a potential risk for your organisation’s IT.
Learning from mistakes?

The fact that unsecured laptops and other devices are still found in taxis, at airports and in numerous other locations and that the private data on them could be the next big headline, should be a wake up call to many government organisations. Unfortunately, that is not the case. Since the beginning of 2012, a Lancashire police force has been fined, three councils: Croydon Council, Norfolk County Council and Cheshire East Council, and they certainly won’t be the last to add their names to the list. Although the cost of a data breach goes way beyond the hefty fines, other measures which need to be taken to provide awareness amongst organisations and their employees have also not been put in place.

Details of the survey

This survey, encompassing 584 UK public sector IT managers from across the country, has been carried out as a joint effort between Sophos and Sustainable Gov in order to assess the current state of data security in the public sector.

Both organisations were keen to discover whether current measures were considered clear and effective enough by public leaders, who have long called for more guidance from those tasked with ensuring data security.

The role of the ICO was also scrutinised, with a great deal of attention paid to how the current system of fines is influencing behaviour.

Out of office

Many public sector organisations do still have traditional stationary workplaces with desktop PCs, however, laptops are gradually becoming the desktop replacement of choice. If you provide laptops to your workers, you have the best of both worlds: with a monitor, keyboard and mouse, a typical desktop workplace can be created; to attend meetings, trainings and other activities not in the immediate vicinity of the your desk, a laptop can be undocked and taken along with you.

1. Source: Ponemon Institute – Cost of a Data Breach Study: United Kingdom, March 2012
Security on mobile devices

When you decide to equip your workforce with mobile devices, no matter whether smartphones, tablets or laptops, it will generally be because you see a way to improve productivity. You also make your users more flexible by providing access to your organisations resources from any location. Before introducing these devices into the workplace, there are considerations to be made as with any computer accessing your network. What additional applications need to be installed? How can the device be secured? How can the access to the network be secured? What about the data on the device? These facts are generally part of a remote working policy which should also include information on acceptable use of the device.

The first question asked in our survey related to such remote working policies and as you can see in Figure 1 below, 64% of organisations do have such a policy in place.

Figure 1. Do you have a remote working policy?

However, even allowing for the fact that a number of organisations do not use any mobile devices, only 32% of respondents who stated that that their remote working policy does include devices such as smartphones comes as a surprise. This could be an indication that the policy needs to be updated or that the risk is underestimated.
Our suggestions

**Review your policy and ensure that it still fits the way your staff work.**

- Are employees using devices you have not taken into consideration?
- Are you aware of what data employees have on their smartphones and other mobile devices?
- Do you have an appropriate use policy to define private usage of corporate devices?

A mobile device *per se* is more personal than an office computer. Even when devices are owned by the organisation, the user will always be the administrator and therefore has to be fully aware of potential security risks.

The biggest mistake many of us make, is that we still look upon smartphones as phones, when in fact they’re small computers and ought to be handled as such. If you have a consultant or external employee working in your office for a few months, you would only give them access to certain areas of your network to do their job. You probably also have stipulations about whether employees can take company documentation home with them or not. But do your employees’ personal smartphones or tablets have full corporate access without the usual security features in place? And even for the devices you own, can you really be sure that they are not breaching many of your security policies on a daily basis?
Data Protection in the UK Public Sector The Changing Face of Data Security

Legal and compliance regulations
The survey found that 48% of respondents only improve their data security because of the legal obligation to do so.

Whilst it is important to have a strong legal imperative to encourage those tasked with handling and storing government data to provide adequate safeguards, this figure may be indicative of a concerning lack of motivation on these individuals’ own behalf. The legal obligation should provide a natural basis for procedures, but the drive to protect data should come from within. It should be pressed externally, but the benefits of keeping data secure should be emphasised and reiterated in order for individuals to fully take on board the essential lessons.

Figure 4. How clear and accessible do you find the compliance regulations in the UK?

- I do not think that the obligation to protect data is clear to businesses 22%
- The obligation to protect data is clear, but I do not get clear guidance on how to achieve this 44%
- The obligation to protect data and the guidance given on how to accomplish it is very clear 33%
- No answer 1%
Key drivers to act on data security

When we read of the possible fines for a data breach, you would probably assume that they would be an adequate motivator to put effective data security policies in place. Our study has shown that this is not the case. The legal obligation (48%) and possible reputation damage of a data breach (35%) are by far the strongest drivers to act on data security. The 4% who responded that their IT staff think it is important should not be neglected. The most recent study by the Ponemon Institute “The Cost of a Data Breach UK, 2011” published in March 2012 has shown that organisations who have personnel responsible for IT security, such as a Chief Information Security Officer, or CISO, have both a reduced risk of a data breach and if a breach cannot be avoided, they at least have significantly lower costs as a result of it.

Figure 5. What is the biggest driver to act on data security in your organisation?

Building awareness

Educating staff about the appropriate use of mobile devices and what to consider when handling sensitive data can help but taking protection out of their hands could be the only viable option for government organisations dealing with personal records. Trusting employees is not a reliable way to ensure data security although a good amount of common sense does help. Data protection needs to be transparent for the organisation but should not hinder users in their work.
Our survey showed that there are very different approaches. The classic classroom type of training – or online webcasts if staff are distributed geographically – is still the most popular method and one of the most effective but, as with popular news channels, repetition is the key to getting your message across. Therefore, it is important to train staff regularly on the most basic measures they can take personally to keep your data safe. Also the use of materials such as posters and screen savers can add to the effect.

Organisations dealing with personal records do often include a clause in the employment contract of their employees to enforce a legal obligation which when not adhered to can carry consequences.

What the technology community can do

Responses have shown that many organisations are fully aware of the obligation to protect their data but need more guidance on how to do so. The technology community should see this as a their opportunity to educate potential users. The 42% of respondents who answered that they want technology to enable their workers to use their own devices securely shows that an automated approach would be preferred.

Figure 6. What can the technology community do to help you most?

- Help develop regulations and compliance to be more accessible and clear 28%
- Give me technology that enables users to use their own devices securely 42%
- Help me build awareness of the importance of security and IA 23%
- Supplement my resources – come in and deploy controls for me 5%
- No answer 2%
Encryption is a typical example of security technology which can be implemented to enforce data security policies and if it is done right, it doesn’t require input from the user. In the case of lost or stolen devices, the data on them is still safe and therefore inaccessible to the ‘finder’. But security goes beyond the device itself in today’s society of information workers. By exchanging data with other people – be they internal or external – data protection needs to be enforced in the same way. Every file transferred to a USB stick or SD card could become a potential loophole in data security and therefore the focus needs to be placed on securing the data and not just the device. The same can be said for the use of other storage media and especially for cloud storage which is often in use without the knowledge of the employer.

**Summary**

The results of the survey are clear: public leaders are calling for greater assistance on how they should manage and refine their data protection policies. ICO fines have been issued to many individuals, but their purpose is often aggravating or misconstrued by those on the receiving end.

There is a growing acceptance that these fines are impeding the progress of an innate data protection culture. While the fines have often been successful at least in getting the message across, they are a decidedly blunt instrument which can lead to conflict.

Experts seeking to empower the public sector with greater knowledge of data security procedures are now calling for an end of the blunt measures. In their place, education would be prioritised, with strong policies set in place and all employees from management level down taught the benefits of keeping data secure and the risks of failing to act. A more self-regulating, holistic solution to the problem could then be forged. Also technology solutions need to be deployed which take over the task of securing data in areas where personal records could be put at risk through negligence.
Simple tools to improve data security awareness

These IT Security Dos and Don’ts are simple tools for every organisation to improve awareness about data security. Our customisable security training programme provides you with all you need to keep your data safe.

- Program launch guide
- Employee handbook
- Email Series of 10 Tips
- Poster Series of 10 Tips
- Online Videos
- Password Quick Tips
- Launch Announcement
- Buy-in Documents

You can find out about our IT Dos and Don’ts under [www.sophos.com/staysafe](http://www.sophos.com/staysafe)

To learn more about encryption products please visit [www.sophos.com](http://www.sophos.com)