

An ounce of prevention is worth a pound of cure

By Martin Blackhurst, head of IT security at Redstone Managed Solutions

Posted Tuesday 2nd March, 2010

Martin Blackhurst, head of IT security at Redstone Managed Solutions.

Public sector managers are living in challenging times when it comes to preventing data loss for their organisations. Compliance with security regulations has become a real headache for managers within the NHS, local and central government and other public sector bodies trying to manage their complexity whilst at the time battling with the ever growing pressure to reduce IT spending.

Council IT departments alone are under heavy pressure to reduce costs. The latest SOCITM IT Trends Report forecasts that capital spending will fall by 20 per cent in 2010, with central IT spend falling by eight per cent. This is the largest decrease since Socitm began producing the report in 1986.

But can we really afford to cut corners on data loss prevention? The answer is definitely not. It is now more critical than ever for public sector organisations to focus their attention on data security because not only is it their responsibility to ensure that sensitive information isn't leaked to the outside world, but they will suffer heavy penalties for not doing so.

New powers, designed to deter personal data security breaches are expected to come into force on 6 April 2010. The Information Commissioner's Office (ICO) will be able to order organisations to pay up to £500,000 as a penalty for serious breaches of the Data Protection Act (DPA). A University Hospital NHS Trust recently found in breach of the DPA would have been given far more than a wrap on the knuckles after April this year, when an unencrypted laptop containing sensitive personal information was stolen from one of its vehicles.

This begs the question, why were so many records downloaded, unencrypted, onto laptops in the first place? Furthermore, since 2008, NHS organisations have been able to procure free encryption, as a result of a directive & bulk purchase of licenses by CfH, the agency responsible for the NHS National Programme for IT. The new Data Protection Act will be a real wake up call for organisations to more carefully examine their IT security strategy and take action.

There is added compliance pressure from other regulations, such as the official IT security standards set by the Government's Code of Connection (CoCo), the Regulation of Investigatory Powers Act 2000 (RIPA) which regulates the disclosure of communications data and access to electronic data, and the Freedom of Information Act 2005 which is diametrically opposed to the requirements of CoCo and RIPA.

There can be no shortcuts when it comes to protecting data and it is up to business managers within public sector and private organisations to understand and act on the risks involved rather than delegating the task to the IT department.

One of the major issues when faced with tackling data loss prevention is working out exactly where the data is that you need to protect. This is a huge task for many public sector organisations which have numerous departments with data saved on numerous servers on different types of platforms. Each department may have its own data which is accessed in various ways by office based or mobile workers. Furthermore, the shift towards closer integration and data sharing between public sector services has cast the net of access to data even further beyond the realms of the organisation that originally 'owned' the information.

So what steps can be taken to ensure that new and existing compliance is met and a high standard of data loss protection is in place?

1. Security Policy - Critically, a business manager needs to work with the IT department to ensure that there is a security policy in place that outlines the acceptable usage of data in and out of the organisation. There needs to be clear direction for each employee on their level of access to data and the level of usage, for example whether data can be downloaded onto USBs, laptops or whether data can be pasted into an email or accessed out of hours. Communication of the policy should become part of the induction process and most importantly regular workshops need to be held with employees to ensure that the users are educated in a positive way to avoid future transgressions.
2. External threat prevention - It is imperative to make sure that there is adequate malware protection and intrusion detection in place to prevent individuals outside the organisation trying to access any data.
3. Encryption - The security policy needs to enforce encryption if data is copied onto removable devices such as USBs, and CDs, or stored on laptops. Policy should also dictate who within the workforce can be permitted to copy or manipulate information outside of the realms of normal use.
4. Data classification - By discovering what data you have it is then possible to classify it by its content as being highly confidential, confidential or for everyday business use. A consultancy provider can help an organisation to classify their data and discover their data through specialist data discovery tools. Once data has been classified it is easier to apply data loss prevention policies for different types of users.
5. Identity and Access Management - Data security should be closely tied with an identity and access management solution which allows a business manager to set the rules on who has access to what data in the organisation. By setting specific rules, it will manage any changes in the workforce in relation to data access, e.g. if an employee leaves the organisation or changes role.
6. Consolidation - With various types of software and hardware required for effective data loss protection from both external and internal threats, it is often the case that an organisation may need to approach multiple suppliers. It can be more beneficial and cost effective to work with technology solution providers who can provide more objective recommendations and a better understanding of the public sector's requirements.

Data loss prevention is unquestionable. In the face of compliance, budget cuts and multiple IT systems it can seem like data security is too big a mountain to climb. But by investing some time in your IT security strategy, consulting with technology solution providers who understand your constraints and ensuring that the whole organisation is on board with security policies it is certainly an achievable goal.

Peter Wenham, who is an IA consultant and the Leader of the Crime & Security Forum of the Communications Management Association (CMA) gives the following tips to tackling data classification.

1. Understand what data you have - by holding well constructed workshops with senior management led by an external consultant experienced in Information Assurance (IA) matters.
2. Find out where the data is - managers of each department need to discuss with their staff where the organisation's data is located, for example, on file servers, laptops, databases, email, or desktops, with a view to identifying duplications and copies (known or otherwise).
3. Identify the sensitivity of the data - whether it is public, protected, secret or top secret and decide who should have access to it.
4. Set standards across the organisation - by setting standard definitions of roles within the organisation it makes it possible to identify consistently the grading of your workforce and each individual's access rights to data. For example, some employees may be able to access data, but not edit, others may be given no access at all.

5. Conduct a final gap analysis - to ensure that the new grading system of the workforce matches up with the existing access controls.

6. Work out a plan of action - whereby the IT department could look to tightening up its security strategy and senior management may need to provide a budget to enable the IT department to generate better data access controls.

View original article at <http://www.gpsj.co.uk/view-article.asp?articleid=186>