



# Safe and sound

Cloud computing, workforce mobility, consumerisation and automated attacks are all increasing the security risks to government data and systems. Find out how to stay one step ahead.

## Top 10 tips for improving data security

1. Assume your organisation is a target and has already been compromised
2. Keep an up-to-date list of known vulnerabilities
3. Encrypt data on mobile workplace devices
4. Participate in a security community and share data on attacks
5. Undertake a data classification exercise to support a tiered approach to security
6. Audit existing security tools to determine their effectiveness and how they support regulatory compliance
7. Be ready to deploy new security tools, such as network forensics solutions, as threats become more difficult to detect
8. Engage a CLAS level consultant to help update existing information security strategy to reflect new risks associated with consumerisation of IT and cloud computing
9. Block spoofed email addresses with a sender policy framework
10. Deploy security solutions that detect and deter automated attacks

Budget-strapped public sector organisations are finding it harder to protect government information and systems from increasingly sophisticated and frequent security threats.

As well as the having to defend themselves against long-standing cyber threats, for example Trojan horses, spam and viruses, public sector organisations now face the added challenge of addressing the security risks that come with new ICT trends, such as example consumerisation and cloud computing.

Andy Clough, Public Sector Client Director, at Computacenter, comments: "Government ICT departments are having to mitigate more threats with less resource, which means there is a greater risk of system security being breached and sensitive data landing in the public domain."

Internet security specialist Symantec detected 286 million new threats in 2010<sup>1</sup> while the Imperva 2011 Web Application Attack Report (WAAR)<sup>2</sup> revealed that an average web application now experiences 27 attacks per hour. This goes up to 25,000 attacks an hour if an automated approach is used. In 2008, 87 per cent of organisations reported suffering either just one or a few malware infections for the entire year.<sup>3</sup>

Such attacks are increasingly being driven by the commercial value of data as well as political motives. For example, the Serious Organised Crime Agency had to take its website offline in June this year after a denial of service attack by a computer hacking group, which is reported to have launched an anti-government campaign.<sup>4</sup>

## The risk from within

Despite their sophistication and proliferation, external cyber attacks are not the greatest security risk facing public sector organisations. According to an IDC survey the top security threat cited by government organisations is employee error or accidental loss of sensitive information.<sup>5</sup>

This concern is well-founded: a study by data security firm SailPoint found that nearly a quarter of UK employees would be willing to sell proprietary data on the Internet.<sup>6</sup>

To deter such criminal activity, organisations need to consider strengthening the security measures imposed on workplace ICT. For example, pre-configuring devices to prevent data from being downloaded onto USB flash drives or implementing a data loss prevention solution that can detect if sensitive information is sent via email, for example to a personal mailbox.

## Encrypt it or lose it

As well as preventing pre-meditated information breaches, public sector organisations must also establish safeguards to address that age-old problem of staff losing devices.

Andy Goddard, Practice Leader for Workplace and Collaboration, comments: “Although flexible and remote working strategies provide public sector organisations with an opportunity to save time and money, they also introduce increased security risks as more devices – and therefore – data is taken beyond the firewall.”

The public sector has already racked up a disquieting data loss record during 2011, with NHS organisations, schools, councils and housing authorities all falling foul of the Information Commissioner’s Office (ICO) due to mobile workplace ICT devices – and their data - being stolen or mislaid.

The majority of these breaches involved unencrypted data stored on laptops or USB drives. This leaves government organisations open to regulatory action by the ICO, which, as of April, can now carry out spot checks and issue fines of up to £500,000 for any organisation found guilty of data breaches.

Colin Williams, Computacenter’s Networking and Security Practice Leader, comments: “Encryption technologies are always evolving; consulting best practice advice provided by the likes of CESG or the Federal Information Processing Standards will help public sector organisations determine the right level of protection for their data. When implementing encryption, ICT departments need to prevent any interruptions to existing data flows and put processes in place to streamline the management of encryption keys.”

## Cloud and consumerisation change the rules

The solutions used for encryption and other information assurance strategies will increasingly need to be platform agnostic. The trend towards the ‘consumerisation of IT’ - where users either bring their own devices into the workplace or have a choice of laptops or smartphones from a managed catalogue – means that public sector ICT departments will need to protect data across a wider portfolio of devices and against a larger number of threats.

According to Gartner, through 2013, 80 per cent of organisations that adopt ‘bring your own PC to work’ programmes will see their botnet compromise rates increase by 100 per cent or more.<sup>7</sup>

“Despite the industry hype very few organisations outside of the technology sector have yet to embrace this ‘bring your own’ approach but it’s a trend that can’t be ignored. If the analysts have got their predictions right, it will become increasingly prevalent, which means more changes to workplace security policies and processes,” comments Andy Goddard.

The rise of cloud computing will also impact existing security policies and processes. Although there are plans afoot to set up a dedicated government cloud environment, many public sector organisations may decide in the interim to migrate commodity services, such as email, to a third-party cloud platform in a bid to cut their operational spend.

“Hosting data in public or private clouds means government ICT departments become reliant on the security measures of an external provider,” comments Andy Clough. “Organisations need to ensure they work with a provider that understands their regulatory and reporting requirements and applies the right level of security controls, especially around employee access rights to sensitive data.”

## Setting the security parameters through data classification

To understand the controls needed – both for internally and externally hosted systems – ICT departments must first understand the data involved.

A data classification exercise using automated software discovery tools will enable organisations to assess both structured and unstructured information stored across their infrastructure.

“Data should not only be categorised based on its criticality but also according to the access permissions, encryption and retention periods that are required,” comments Colin.

The classification results will help ICT departments define and deploy appropriate security measures for different data sets and set the right parameters for external partners, such as cloud providers.

For example the Government Connect Secure Extranet (GCSX) – a private wide area network (WAN) that enables information-sharing between local and central government organisations – demands that log data is retained for six months.

## Sticking to the basics

Data classification is just one way in which public sector organisations can improve their information assurance strategy. There are a number of other simple steps that can be implemented – without the need for extensive capital expenditure.

According to Australia’s Defence Signals Directorate (DSD), which analysed the attacks launched against Australian government networks, 85 per cent of network vulnerabilities can be addressed through these relatively straightforward defences:

- Keep applications patched
- Use the latest version of applications, in particular Flash, Acrobat PDF viewer, Microsoft office and Java
- Patch operating system vulnerabilities
- Minimise the number of users with administrative access to systems
- Whitelist applications.

“Although this advice probably seems incredibly simple, for under-resourced public sector ICT departments even getting the basics right can be a challenge,” comments Andy Clough.

Only nine per cent of public sector organisations have more than 10 members of staff working on data protection duties compared with 31 per cent in the private sector.

## Tapping into additional resources and skills

Despite the lack of resource, government organisations demonstrate a good understanding of the data protection measures that need to be followed. In an ICO survey, 60 per cent of public sector respondents spontaneously cited information security as a key obligation of the Data Protection Act compared with 48 per cent in the private sector.<sup>8</sup>

“Public sector ICT departments know what they need to do in terms of information assurance, but often lack the skills, resources and tools they need to put best practice into action,” comments Andy Clough. “By working with an external partner, public sector organisations will be able to establish an effective but economical strategy for securing data and systems.”

Although financial considerations are increasingly part of the security equation, some public sector organisations will have to accept the need to spend to save if their existing tools are insufficient. According to Gartner, the cost of mitigating a data breach is likely to be vastly greater than the cost of preventing the breach beforehand — perhaps by a 70-to-1 margin.<sup>7</sup>

“Despite the current austerity measures, information security must remain a key priority for the public sector. Failure to commit sufficient resources or deploy adequate tools will not only result in increased operational costs but also damaging data breaches and a loss of public confidence,” comments Andy Clough.

## Further Information

Unlock the full value of your business information with optimised security and storage strategies that reduce risk and cost. Find out more:  
[http://www.computacenter.com/services/consult\\_and\\_change/secure\\_information/](http://www.computacenter.com/services/consult_and_change/secure_information/)

### Footnotes

- 1 Symantec Internet Security Threat report 2010, <http://www.symantec.com/business/threatreport/index.jsp>
- 2 [http://www.publicsecurityportal.com/publicsecurity\\_news.asp?articleid=266571&arttitle=Shocking%20level%20of%20automation%20in%20cyber%20attacks](http://www.publicsecurityportal.com/publicsecurity_news.asp?articleid=266571&arttitle=Shocking%20level%20of%20automation%20in%20cyber%20attacks)
- 3 2008 Information Security Breaches Survey, Department for Business, Enterprise & Regulatory Reform
- 4 <http://www.zdnet.co.uk/blogs/communication-breakdown-10000030/soca-admits-ddos-attack-claims-secure-info-safe-10022788/>
- 5 Government Insights, June 2011, IDC
- 6 <http://www.v3.co.uk/v3-uk/news/2097039/nearly-half-brits-willing-breach-company-security-study#ixzz1TIBGNQwx>
- 7 Predicts 2011: Infrastructure Protection Is Becoming More Complex, More Difficult and More Business-Critical Than Ever, November 2010, Gartner
- 8 Annual Track 2010, Information Commissioner’s Office