

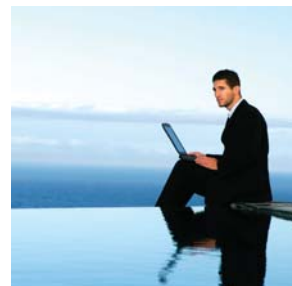
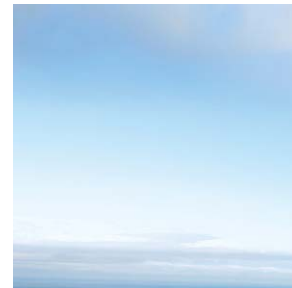


**CLEARSWIFT™**

Simplifying content security

## Information Assurance: A Game of Hide and Seek in the Public Sector

# Clearswift IA08 Digital Survey Results



## The Insight: IA is Broken

Recent research from Clearswift and other security technology leaders like Symantec suggests that, when it comes to IA in the public sector, there's a major fault line emerging between operational objectives and public expectations - and that we're in danger of permanently harming public trust if we don't do something radical about it.

## The Situation: The Public IA Divide is Widening

On one hand, management appears to be burying its head in the sand, whilst on the other, consumers and the public are demanding more insight and more transparency in the way that important information is managed.

For example:

According to our recent IA research ("IA and Organizational Responsibilities in the Public Sector, 2008"), 54% of respondents – all of whom either work within or for a public sector department – felt that their organisation didn't spend enough time on IA issues.

Whilst, conversely, recent research from Symantec showed that 96% of UK consumers want to be notified if a private or public sector organization loses their data.

At the same time - and more alarmingly, in a separate Clearswift research report ("Worldwide Data Loss Prevention Trends, 2008"), we see that nearly 90% of all IT decision-makers don't believe that the general public should be informed if a data breach occurs, and 60% are unaware of the proposed introduction of data breach notification legislation.

We believe that this 'hide and seek' trend perfectly illustrates the problem of IA today. Corporations and public departments are either concealing or ignoring their IA obligations, whilst consumers and the public are actively looking for support and answers.

## The Result: Ignorance and Incidents

We appear to be hard-wired to treat IA purely as a technology issue but not as a service issue, a communications issue, or a compliance issue. As such, it's become something for IT managers to worry about, and an end in itself.

In other words, IA is not currently a board level concern. This fact is illustrated by our research. For example:

Our IA 2008 Research suggests that almost 60% of senior management understand little or nothing about IA, and that 50% of organizations have discussed IA fewer than four times at board meetings in the past year.

This approach to security is wrong. The role of IA in the public sector is to protect the information that needs to be secured, and safeguard the information that needs to be shared - both internally and externally. This is not purely a job of the 'department downstairs'. It needs to be a directive of the organisation at large so that you're better able to fulfill the requirements and expectations of your public constituencies.

Why? Because in reality, information is everything: it's so much more than mere data. This much is obvious - we all read the 'Al-Qaeda papers on the train' news last week.'

As such, IA is trust; IA is mission-critical. And it needs to be handled with more respect if the pervasive culture of 'mishap expectancy' is to be overcome.

Our IA 2008 Research also suggests that around 70% of organizations actively expect to experience a new IA failure in the next 12 months.

(Was last week's 'papers on the train' story really news in the truest sense? After all, they were handed back to the BBC, not the MoD .... which is surely a sign of public weariness on an IA matter of national security!)

**"Processes, polices, common sence...."**

**"Making IA part of normal everyday business across the Civil Service in a proactive manner rather than in reaction to individual crises"**

**"Work on the right cultural and enviromental improvements - not just the technology"**

Source: IA 2008 Digital Survey

**“Improve the culture; raise up the management agenda”**

Source: IA 2008 Digital Survey

## The Action: IA Mission Statements

In short, we feel that public sector organizations urgently need to align IA with their higher goals. Handling information with respect in order to assure service transparency, quality and security needs to become a bullet point within your department's mission statement.

It's also clear that your employees and colleagues feel the same:

Our IA 2008 Research suggests that around 85% of organizations feel that their IA procedures could be significantly improved; whilst 85% also felt that IA procedures could be improved significantly across the UK government as a whole.

It's only by taking action at board level that IA can become part and parcel of public service delivery.

## The Conclusion: IA is a Mission-Critical Issue. It's a Process, Not a Product

Despite being a product vendor, we realise that IA is not a software patch or a firewall, it's a way of doing things. It's a process that needs to get hard-baked into an organisation's make up.

IA is a mission-critical issue that urgently needs a seat at the board table. It needs to be better defined in terms of process and responsibilities and it needs to shape the way your organisation lives and breathes. If you can do this, it may not help to keep you off the front page all the time - accidents do happen, but it will eradicate the more foolish mishaps and help to restore public faith in your services.

**“Make operational managers understand and be accountable for IA”**

**“Give direction with teeth and inspection programmes with published results”**

**“Make data protection breaches reportable, plus fines”**

Source: IA 2008 Digital Survey

## About Clearswift

Clearswift helps organizations and establishments of all sizes conduct business safely over the Internet.

Our policy-based content filtering and security solutions block bad content such as spam, viruses, malware, spyware and pornography; protect sensitive information by preventing leaks; and prevent time-wasting and abuse by controlling inappropriate use of the Web and social media while eliminating exposure to offensive content.

Clearswift makes it easy to deploy, manage and maintain no-compromise e-mail and Web security across all gateways and in all directions. And our EAL4 accredited military and government solutions protect some of the world's most security-sensitive organizations.

Our technology reflects twenty years of experience across more than 17,000 organizations with a pedigree based upon granular policy management; easy administration; and the ability to combine best-of-breed security tools into powerful, no-compromise defenses.

Clearswift customers use the Internet with confidence.

## Contact Clearswift

### United States

100 Marine Parkway, Suite 550  
Redwood City, CA 94065  
Tel: +1 800 982 6109 | Fax: +1 888-888-6884

### United Kingdom

1310 Waterside, Arlington Business Park, Theale,  
Reading, Berkshire, RG7 4SA  
Tel: +44 (0) 11 8903 8903 | Fax: +44 (0) 11 8903 9000

### Spain

Cerro de los Gamos 1, Edif. 1  
28224 Pozuelo de Alarcón, Madrid  
Tel: +34 91 7901219 / +34 91 7901220 | Fax: +34 91 7901112

### Germany

Amsinckstrasse 67, 20097 Hamburg  
Tel: +49 40 23 999 0 | Fax: +49 40 23 999 100

### Australia

Level 5, Suite 504, 165 Walker Street,  
North Sydney, New South Wales, 2060  
Tel: +61 2 9424 1200 | Fax: +61 2 9424 1201

### Japan

Hanai Bldg. 7F, 1-2-9, Shiba Kouen Minato-ku  
Tokyo 105-0011  
Tel: +81 (3) 5777 2248 | Fax: +81 (3) 5777 2249