



Australian businesses say general public doesn't need to know about security breaches

Clearswift survey reveals Australian IT managers are for data breach notification legislation

AUSTRALIAN BUSINESSES SAY GENERAL PUBLIC DOESNT NEED TO KNOW ABOUT SECURITY BREACHES

Clearswift survey reveals Australian IT managers are for data breach notification legislation

Key results:

- 96 per cent of IT decision-makers dont think the general public should be informed if a data breach occurs; but only 28 per cent are against the introduction of legislation that would force companies to declare a data breach if it occurred
- 48 per cent are in favour of legislation that would make negligent loss of personal information a criminal offence
- 20 per cent of companies have suffered a data loss in the last 12-18 months; 38 per cent more than once
- 48 per cent of IT managers believe their annual IT spend would increase by up to 10 per cent with the introduction of data breach notification legislation

Sydney, Australia 15 July, 2008 A recent survey by content security specialist Clearswift, has revealed that when it comes to data security breaches, 96 per cent of Australian IT decision makers believe that companies do not need to inform the general public. The majority of respondents did indicate that affected customers and partners should be informed (82 per cent) while 63 per cent suggested that regulators should be advised and 35 per cent believe the police should be notified.

Of the Australian organisations polled, 20 per cent had suffered a data loss in the last 12-18 months, and of those, 38 per cent had experienced more than one. Despite the fact that more than 82 per cent of those surveyed said that data loss/data breach was a very important or imperative issue to their organisations, the research indicated that they are still not locking down the transfer of sensitive information appropriately. Email is the most popular method of transferring confidential data (85 per cent allow staff to transfer confidential data via email), and yet 39 per cent of businesses admit to losing data via email.

To counter the threat, 81 per cent are aware that their organisation has security measures in place to prevent data breaches or data losses from occurring. However, 16 per cent dont have email content filtering solutions in place, 25 per cent dont have Web content filtering and half dont have encryption solutions. Moreover, more than 30 per cent (31 per cent) dont have a data loss or data breach prevention policy in place and nine per cent didnt even know if they had one.

Following the recent debate surrounding the call for data breach legislation, the research demonstrates the Australian business communitys support for guidelines that would advise on best practice in a data breach or data loss incident. It also highlights that there is still a concerning lack of awareness when it comes to the risks and consequences of data loss - so theres still a big job to be done, said Peter Croft, Managing Director for Clearswift Asia Pacific.

At the same time, the majority of the IT decision makers that we surveyed admitted that while they are prepared, when faced with the prospect of having to air some dirty laundry in public, companies are not always confident they will emerge in a positive light, and feel that potential legislation enforcing disclosure could be expensive, result in a loss of confidence by customers and partners, and create significantly more work for the IT department.

When asked about the likely impact of data breach notification legislation, half of the respondents agree there would be both positive and negative affects on the business. 94 per cent feel it would facilitate a greater understanding among employees of the importance of good security practice, while many anticipate it would also improve overall business practice and increase consumer and stakeholder confidence.

Almost half of respondents (48 per cent) expect that such legislation would increase annual IT spend by at least 10 per cent. Additionally, 75 per cent of IT managers believe any new data breach notification legislation would damage the reputation of their organisation.

While the threat of data loss or breach continues to increase, there are still organisations that have not invested in data security. Respondents

indicated the following as the top three reasons why:

- 18 per cent dont consider data loss prevention to be a priority or feel that they need to protect against it
- 32 per cent trust their employees to follow the corporate policy
- 32 per cent do not have the budget to invest in data loss prevention solutions.

Nearly anyone deploying a DLP solution will eventually want to start blocking traffic. Theres only so long you can take watching all your juicy sensitive data running to the nether regions of the Internet before you start taking some action, said Rich Mogull, analyst and founder of Securosis.

But blocking isnt the easiest thing in the world, especially since were trying to allow good traffic, only block bad traffic, and make the decision using real time content analysis.[1]

"Data leakage is now considered the 4th most serious threat to enterprise IT security in Australia (behind viruses/worms (1), spam (2) and spyware/Rootkits (3)), according to the IDC Australia Security Survey 2008" Said Patrik Bihammar, Senior analyst at IDC Australia and New Zealand.

However, the survey showed that only 29.4 per cent of Australian organisations are currently planning to implement DLP solutions in the next 12 months. The top barriers for DLP investment are usually lack of budget and the belief that solutions are too complex to implement and manage.

Clearswifts content security technology helps companies monitor all content leaving their organisation via email and the Internet, preventing any confidential information reaching the outside world, whether sent accidentally or maliciously. At the same time, Clearswift can protect organisations from spam, viruses, spyware and web-borne malware, as well as help define and enforce policies on acceptable Internet usage.

Data Loss Prevention or DLP is a top of mind issue that companies will be grappling with for the foreseeable future. Companies need to evaluate their current security policies and measures to ensure that they are fully protected. A layered approach to security that monitors all content leaving the business and simultaneously managing multiple outlets is by far the most successful solution, concluded Mr Croft.

-Ends-

[1] Mogul, Rich, Understanding and Selecting a DLP Solution: Part 3, Data-In-Motion Technical Architecture, September 18, 2007, Securosis.com, <http://securosis.com/2007/09/18/understanding-and-selecting-a-dlp-solution-part-3-data-in-motion-technical-architecture/>
<<http://securosis.com/2007/09/18/understanding-and-selecting-a-dlp-solution-part-3-data-in-motion-technical-architecture/>>

About the research

All the above figures, unless otherwise stated are from Clearswift. Total sample size was 208 Australian IT decision makers. Fieldwork was undertaken between March 10 and April 10, 2008. The survey was completed online.

About Clearswift

Clearswift helps organizations 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 worlds 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.

www.clearswift.com <<http://www.clearswift.com>>

