

# Most companies and organisations dont know what their employees are up to in cyberspace

Sixty-five per cent of companies and organisations do not know whether employees have downloaded or made illegal copies of software and around half (46%) do not have clear policies on Internet downloading and software use, according to research by the Business Software Association of Australia (BSAA), which it says exposes organisations to grave risks of viruses, worms, security breaches and legal action for piracy.

Two-thirds (66%) of businesses surveyed do not conduct software audits or check what workers are using, and 41% admitted that they do not know if they are correctly licensed for software used in their organisation.

Even worse, more than a third (36%) of companies and organisations admitted that they do not know exactly how many computers they have.

With this clear lack of management attention to computer use, companies and organisations are effectively leaving their back door open electronically and shows why its more important than ever for organisation to look at implementing Software Asset Management (SAM) practices, Chairman of the BSAA, Jim Macnamara, warned.

The alarming findings came from two online surveys conducted by the BSAA in May which gained responses from 978 companies and organisations of different sizes and in various sectors ranging from education to IT and government.

Mr Macnamara said that separate independent research by Gartner Group reported that where computer use and Internet downloading were not strictly controlled, organisations were highly likely to have illegal software business programs, games and music files as well as viruses, worms, security breaches and technical problems on their networks.

This can be costly in terms of lost productivity and potentially legal costs for copyright breaches, he warned.

Mr Macnamara said the solution for cybersecurity was relatively simple and involved three key steps:

1. Install and use virus protection software on all PCs and network servers;
2. Set up a firewall on servers to protect networks (a computer to screen downloaded material and incoming e-mails); and
3. Conduct regular spot checks and audits of software in use.

Mr Macnamara said having clear policies in place on Internet downloading and software use and regularly checking computer systems are essential in the online age. These policies are all part of having a comprehensive SAM process in place.

He said: Employees download, install and pass around illegal and sometimes dangerous files through ignorance and naivety in some cases, and occasionally intentionally, and it is up to management to have systems in place to ensure computing environments are safe, secure and legal.

The BSAA offers free advice and a wide range of SAM advice and tools for conducting software audits on its Web site [www.bsaa.com.au](http://www.bsaa.com.au).

#####

More information:

Toll-free hotline for public inquiries (anonymously if preferred): 1800 021 143

BSAA Web site: [www.bsaa.com.au](http://www.bsaa.com.au)

The Business Software Association of Australia (BSAA) is affiliated with the Business Software Alliance (BSA), which operates globally in 65 countries. BSAA members include Adobe, Apple, Autodesk, Microsoft and Symantec.

The Business Software Alliance ([www.bsa.org](http://www.bsa.org)) is the foremost organisation dedicated to promoting a safe and legal digital world. BSA is the voice of the world's commercial software industry before governments and in the international marketplace. Its members represent one of the fastest growing industries in the world. BSA educates consumers on software management and copyright protection, cyber security, trade, e-commerce and other Internet-related issues. BSA members include Adobe, Apple, Autodesk, Avid, Bentley Systems, Borland, CNC Software/Mastercam, Internet Security Systems, Macromedia, Microsoft, Network Associates, SolidWorks, Sybase, Symantec, UGS and VERITAS Software.

## Contacts

Pru Quinlan

+61 2 8905 0995

mailto: [pru@einsteinz.com.au](mailto:pru@einsteinz.com.au)