

Beyond compliance: How secure destruction protects competitive advantage, prevents fraud and keeps companies in the news for the right reasons.

It's been a while since the Privacy Act changed the way most Australian businesses disposed of office paperwork in December 2002. You may not have been aware that there are more issues to examine when you decide on how to dispose of paper work in your office than the Privacy Act Alone...

The issues facing business today

The use of paper to record, store and view information has continued to grow despite the explosion in growth of electronic media. Some may argue that the electronic information age has in fact *increased* the amount of paper used. Business today is faced with an increasing compliance burden, driven in part by the rise in identity theft and the subsequent impact on society and its victims.

Under the National Privacy Act that affected so many Australian businesses in 2002, an organisation “...**must take reasonable steps to protect the personal information it holds from misuse and loss...**” and “...**must take reasonable steps to destroy or permanently de-identify personal information if it is no longer needed...**”

Businesses must now address the challenge of ensuring that *personal* information is kept confidential right through its life cycle, from the creation of documents to end of their life cycle when they are destroyed. There is, however, a lot more for business to consider than strictly *personal* information; information that can be categorised as *commercially sensitive* can cause significant damage to a company if it falls into the wrong hands.

The importance of secure handling and destruction of commercially sensitive information

Protecting competitive advantage and intellectual property

The discarded paperwork that a business generates from everyday activities could be potentially harmful in the wrong hands, especially your competitors. When you consider all those discarded phone messages, memos, misprinted forms, proprietary material like discarded procedure drafts, faxes, drafts of tenders, emails that have been printed then read and discarded – all this information has the potential to provide an outsider a snap shot of what the business is doing right now, from who it is doing business with, at what price and how often. Someone who came across this information would not need to be

over endowed with intelligence to put these pieces together and potentially wreak havoc. The only means to minimise the risk that this kind of information poses is to securely collect and destroy it.

Protecting public image

It is very embarrassing and potentially damaging when information gets into the wrong hands.

Some recent examples of this are the uproar over the report of the death of Private Jake Kovco that erupted when a senior Defence Department official allegedly left a CD of the draft report behind in a public computer at a VIP lounge at Melbourne Airport.

<http://www.abc.net.au/pm/content/2006/s1642048.htm>

Another recent incident was when Channel 7 revealed information from medical records that were allegedly found in the gutter outside a Melbourne clinic.

<http://www.abc.net.au/news/stories/2007/08/27/2016878.htm>

Clearly, the theft of sensitive documents or their accidental discovery can cause huge public embarrassment for companies and become a real public relations nightmare. Damage to a company's reputation and credibility from these incidents can be severe, from impacting on profits to declining share prices.

Prevention of identity theft

Identity theft occurs when someone takes someone else's name, Tax File Number, credit card number, drivers licence details or some other piece of information without their knowledge to commit fraud or theft. The consequences of identity theft can have catastrophic consequences for its victims, ranging from having to legally change names to spending years trying to clean up messy credit fallout. In Australia alone, identity theft was estimated to be worth between AUS\$1billion and AUS\$4 billion per annum in 2001.

'Skip diving', 'skip raiding' or 'dumpster diving' has traditionally been the prime source of personal information for identity thieves. A strong disposal policy and secure collection and shredding of personal information is the best way to minimise the risk of identity theft.

Prevention of fraud

Could someone at your organization write a password or Personal Identification Number (PIN) on a sticky note? Could they put a faxed purchase order to one of your suppliers for goods and services in the recycling? Could they ever accidentally put a pre-printed cheque that was mis-printed in the bin? If they could, then potential fraudsters could hack security systems with the PIN, place fraudulent orders with your suppliers and literally write a cheque for themselves. Having checks and balances in place to ring alarm bells if your business becomes the victim of fraud is important, but all too often significant damage can be done before anyone realizes what is happening. Fraud like this can go undetected for days or weeks, by which time it becomes difficult to catch the perpetrators.

Recycling as an option

Recycling is not seen as a legitimate means to securely dispose of sensitive material. Scrap paper is worth the most if all the white office paper is sorted from the cardboard and other recyclable material. There is no chain of custody in the recycling process and putting sensitive information out with the recycling puts it at risk of being manually sorted by employees of the recycling company who are potentially non security checked and without training in protecting sensitive material. The transport of recyclable material is generally not secure and with vehicles parked in the street overnight, along with recyclable material sometimes being stored for some time in an unsecured manner prior to being recycled, the risk of information falling into the wrong hands is increased.

The Solution: Secure Destruction

Most businesses now acknowledge their obligations to keep confidential sensitive information, both that which relates to private individuals and to the companies themselves, implementing programs to securely destroy such material. 'Secure destruction' has 2 distinct steps; firstly, the information to be destroyed is collected in a secure manner, with a chain of custody from the collection point to the destruction point and secondly, the information is destroyed so as to be unrecognizable. These 2 steps are not without their challenges.

Capturing the hearts and minds of the people: Planning and implementing a secure destruction program

Generally, an organisation's privacy policy will contain a statement largely similar to or having the same meaning as **"Our company takes reasonable steps to protect your personal information from loss, misuse, unauthorised disclosure or destruction"** which is consistent with the requirements of the Privacy Act. According to the Act, paper documents containing personal information at the end of their life cycle must be destroyed or permanently de-identified.

Once this has been enshrined in policy, it is up to management to provide the tools for the organisation to comply with the policy. Once an organisation has determined what means to use to destroy or permanently de-identified end-of-life paper documents, it must then go about ensuring compliance.

Communicating the need for secure destruction

It is important for everyone in the organisation to take personal responsibility for ensuring that confidential information is securely destroyed. Many employees will be familiar with the problem of identity theft; some may know victims or be victims themselves. It's the other areas of commercially sensitive risk that may need to be clearly explained; things like the consequences of writing PIN information down, what can happen if the company's purchasing procedures are made available to the unscrupulous outside world via purchase orders and how the company's competitive advantage needs to be protected by destroying pricing information.

To communicate the need for secure destruction and make compliance easy for all employees, providing simple tools will be very helpful:

- Make secure destruction part of the induction program for new employees so the culture of secure destruction is ingrained in new employees from the moment they commence employment.
- Update employee manuals to reflect your company's procedures relating to how sensitive information is destroyed and exactly what sort of information needs to be destroyed. Ensure that the individual responsibility of the employee to destroy sensitive material is clearly explained.
- Make secure destruction an item on (or a reason for) a meeting so employees can be made aware of the obligations the company has to the Privacy Act and to its stakeholders to destroy confidential, commercially sensitive and personal information. The personal responsibility everyone in the organisation has to comply with the company's policies and procedures that relate to the destruction of such material can also be stressed to employees at the meeting, as well as an explanation as to exactly what sort of information needs to be destroyed.
- Place secure containers at convenient points throughout the office to collect the information that is to be eventually destroyed.
- Place posters on notice boards and in common areas to remind all employees of their obligations to securely destroy information. Meal rooms and above collection points are a good area to place such information, as is at network printers (where a lot of this information is produced).
- Use memos, internal email, intranet or company newsletters to reinforce the secure destruction program.

Deciding on the disposition method

There are generally 2 options to look at when deciding on how to finally destroy the information collected from the offices of the company. In house/onsite shredding or outsourcing using a company that provides a secure destruction service.

In house destruction

Destroying material in house has the advantage that so long as the process is sound, it is unlikely for anything to leave the site intact, reducing the risk posed by improperly disposed of information. However, the following issues can occur when a company decides to do its shredding on site:

- **Some information should not be trusted to employees for disposition.**
Obviously any information about payroll and legal affairs should not be put into the hands of low level employees for disposition. Competitive information too, like customer lists and pricing schedules should also be protected from them as well. Employees of the company are the ones with the easiest access to this information and are also the ones who are most likely to realise its value to competitors.
- **Planning and implementing a shredding operation can be difficult.**

When planning an in house shredding operation the question of “do we centralise the operation or provide shredders in the offices?” involves 2 costly alternatives; (1) being the purchase, maintenance and eventual replacement of shredders in every office (even if multiple ‘communal’ shredders are used) and (2) being the cost of a big shredder, the staff to run it, the maintenance on it and the use of valuable space to house it. Company funds may be better spent elsewhere.

- **Maintaining a ‘chain of custody’ can be difficult.**
Secure areas will need to be set aside to store material before they are shredded. If secure areas cannot be found, exposed material presents a security risk.
- **Shredding is hard work.**
The professional staff in an office may be unsuited to the dirty, noising task of shredding.
- **What business are you in?**
It’s not the shredding business. Shredding in house can distract employees from the core activities of the business. Company resources may be better directed to areas where they can produce profit for the company.

Outsourcing

Using an outside company to manage your paper destruction needs takes destroying information out of the hands of low level employees who probably should not see it, it eliminates the need to implement and plan for the equipment required to do the shredding, it allows the integrity of the chain of custody from collection to destruction to remain intact, office workers are spared from the undesirable task of shredding paper and it allows the company to concentrate on core activities.

A company that provides secure destruction will be able to provide:

- Lockable destruction bins.
- Secure vehicles for the transportation of the materials.
- A secure site to hold materials before it is destroyed.
- A means to destroy or permanently de-identify information.
- An environmentally friendly program to recycle the material after destruction.

What to look for in a potential supplier of destruction services

With so much at stake in maintaining the confidentiality of personal and commercially sensitive material, it makes sense to place whoever is entrusted with the task of providing the service to a degree of scrutiny. When choosing a provider of destruction services ensure that:

- The employees of the provider sign confidentiality agreements to protect their client’s information.
- The employees of the provider undergo a pre employment and ongoing criminal history checks; any convictions for fraud, theft and larceny prohibit an employee from working with sensitive material.
- The employees of the provider wear their company’s uniform and display a photo ID badge at all times so their clients can more easily identify them. The

company's vehicles and equipment should be clean, neat and tidy. The company's visual appearance should inspire confidence and project a professional image.

- The company can demonstrate a strong chain of custody starting at the collection point and ending with the destruction of the material; they should have good quality, clean and secure lockable bins, secure enclosed transport vehicles and a secure facility to hold and destroy the information.
- The company has written procedures on how to maintain the security of its client's information and the staff of the company should be trained to maintain the secure chain of custody.
- The company should be able to provide its clients with certificates that detail what was destroyed, where it was destroyed, when it was destroyed, how it was destroyed and who destroyed it.
- The company should be able to demonstrate long term financial stability, and have adequate public and professional indemnity insurance in place.
- The company should be able to provide references from current clients that verify the quality of the service provided.

Choosing a secure destruction provider follows the classic rule: you get what you pay for. The cheapest provider may not be the right choice. Carefully examine all potential providers on all of the above points before making a choice on who handles your sensitive information.

Conclusion

With information security becoming a critical issue facing top level executives and the very real threat of what is leaked today becoming front page news tomorrow, there is now more than ever an impetus towards ensuring commercially sensitive and personal information is properly disposed of at the end of its life cycle. Aside from the necessity of compliance with legislation, a secure destruction program with the broad support of all employees and officers of the company from the board room down provides the company, its employees and stake holders with best protection possible against the mishandling of information at the end of its life. With an effective secure destruction program, all those associated with the company - from the general public, employees and shareholders – will have confidence knowing that information that is potentially damaging to them personally and to the company is being protected using secure best practices.