

How You Can Protect Your Business from Security Breaches and Fraud



Making sure
it's secure.™

The news reports regularly on information security breaches. In fact, the number of breaches and associated damages – in monetary penalties, and to customers and business reputations – continues to rise each year.

The following statistics are surprising and frightening, but true:



27% of security breaches experienced by Australian businesses are caused by simple human error.¹

46% of breaches are caused by malicious attacks.²



The average organisational cost of a data breach to Australian businesses is \$2.8 million.³

One estimate puts global business losses due to identity theft at the equivalent of \$260 billion.⁴



A 2014 study by EY, found that more than 1 in 8 executives in Australia's largest businesses experienced a significant fraud in the past two years.⁵

Every business needs a plan to protect confidential information.

It's likely you have sensitive information in your files that includes names, addresses, medical information, credit card and other account data. Unless you take steps to properly protect this information, you can open to the door to loss, identity theft and even criminal fraud. And today, it's more than just a good business practice to protect sensitive data – it's the law. A sound data security plan should include these five essential elements:

- ✓ **Take stock:** Establish what types of confidential information your business holds.
- ✓ **Scale down:** Keep only the information you need for your business. The Australian Privacy Principles dictate that personal information should only be gathered and used for legitimate purposes and should not be kept beyond its useful life.
- ✓ **Lock it up:** Make sure information you hold is kept secure at all stages of its life, whether in electronic or hard copy.
- ✓ **Plan ahead:** Create a plan in the event a security breach does happen.
- ✓ **Destroy it:** Shred confidential paper documents when no longer needed. Make sure you use a secure and documented shredding process conducted by security experts.

The Office of the Australian Information Commissioner has published extensive information and guidance on information security and compliance with the Australian Privacy Principles on its website oaic.gov.au.

For further information on how Shred-it can help you stay secure, contact us at:

1 800 012 012 | shredit.com.au

Make Shred-it Your Partner Against Security Breaches



Making sure
it's secure.™

Big business or small, in any industry, one of the best moves you can make to protect your business is to work with a professional information destruction company. It's important to make sure the paperwork, hard drives and other confidential materials you discard won't find their way into fraudsters' hands, and secure disposal of that information is key.

- ✓ Shred-it's confidential destruction service offers a secure chain of custody for your documents and data, from the moment you place them in the secure container until they're destroyed.
- ✓ As the world leader in information destruction, Shred-it's security experts will help to keep your business compliant with your industry's regulations, protect you against identity theft, and help you maintain your good reputation with customers.
- ✓ Shred-it uses industrial shredding equipment to ensure your documents and data can never be reconstructed.

Take these additional steps to safeguard your business.

Here's what we advise our clients in order to guard against fraud and protect their reputations.

- ✓ **Stay informed:** Learn about current laws and legislation that impact your business, and how to stay compliant. Visit shredit.com.au/resource-centre, for the latest legislation fact sheets, and sign up to receive automatic updates.
- ✓ **Establish a security plan:** Make sure you have formal security policies in place.
- ✓ **Educate and enforce:** Your employees need to know and follow your information security policies. Update employees on a regular basis and post your policy and guidelines around your workplace.
- ✓ **Limit access:** Only authorised personnel should handle confidential information.
- ✓ **Create a retention policy:** Determine which documents you must keep and for how long. Clearly mark a destruction date on all records in storage.
- ✓ **Eliminate risk:** Introduce a "shred-all" policy for ALL documents (confidential/sensitive and general) so that employees don't have to decide what is – or isn't – confidential.
- ✓ **Partner with Shred-it:** Our business is to make sure that no one knows yours.

When it comes to protecting your confidential information, the security experts at Shred-it can help you assess security risks and put together the processes your workplace needs to keep information safe.

Sources:

- 1 Ponemon Institute LLC/IBM, 2014 Cost of a Data Breach Australia
- 2 Ponemon Institute LLC/IBM, 2014 Cost of a Data Breach Australia
- 3 Ponemon Institute LLC/IBM, 2014 Cost of a Data Breach Australia
- 4 U.S. Small Business Administration 2013, How to Prevent and Detect Business Identity Theft
- 5 EY, Overcoming Compliance Fatigue, 13th Global Fraud Study

For further information on how Shred-it can help you stay secure, contact us at:

1 800 012 012 | shredit.com.au