

2015
State of the Industry
Information Security
Australia



Making sure
it's secure.™



Table of Contents

1	Introduction
2	Situation Analysis
4	Security Tracker: Infographic
5	Hot Topics in Information Security
7	Best Practice Tips
9	Ask the Expert
11	Recent Changes to Privacy Legislation
14	Summary

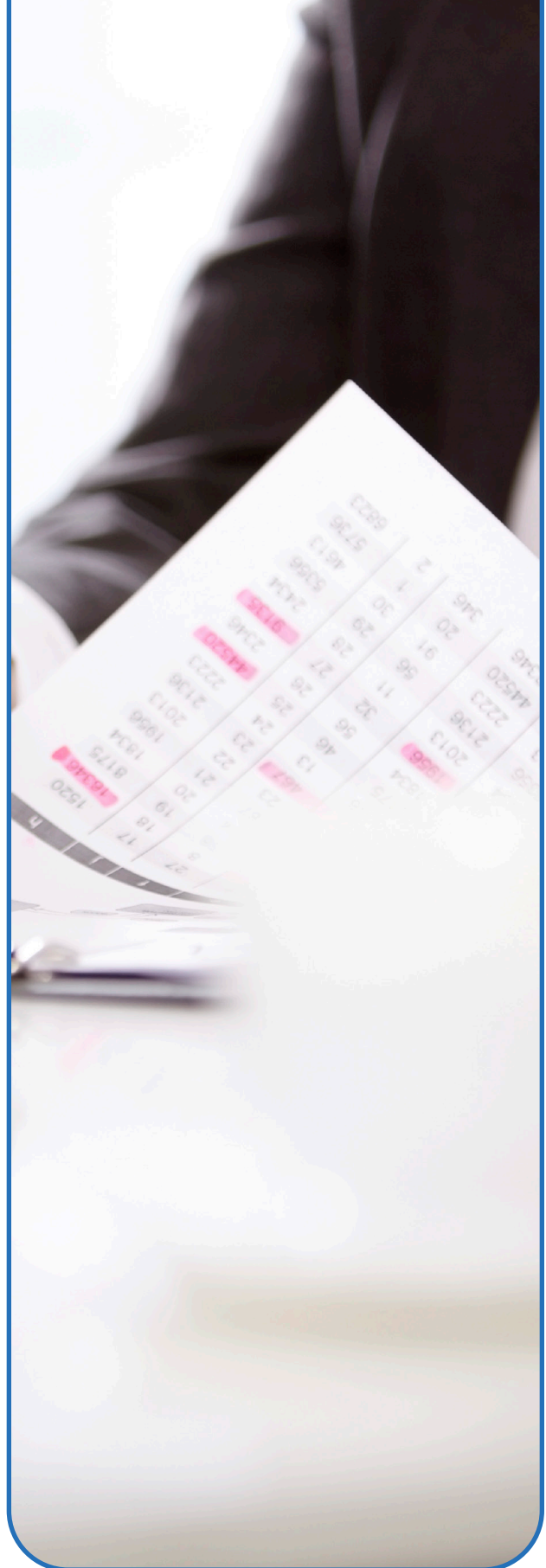
Introduction

Welcome to Shred-it's inaugural State of the Industry Report for Australia. This is a report that analyses industry trends associated with document destruction and information security across organisations of all sizes. Its focus is to highlight the danger areas that are often overlooked, share advice on policies and procedures and provide recommendations to improve information security practices.

In the coming pages, you will find an overview of the findings from the recent Shred-it 2015 Security Tracker, a survey that was conducted for the first time in Australia in May, 2015. This is an independent research study commissioned to gain insight into information security awareness, policies and procedures among SMEs and larger organisations throughout Australia. Although these two reports are firsts for the Australian market, Shred-it has been responsible for these in-depth reports and analysis for several years across the globe including North America, the UK and Germany.

The 2015 Security Tracker reveals the worrying trend of organisations, large and small, not having the right policies and protocols in place for both storing and disposing of confidential information. However, as is often the case, it is most prevalent in the smaller sized organisations that have fewer resources, time and knowledge to implement comprehensive document disposal practices.

The information within this report shows that in addition to being good security practice, a focus on information security makes sound business sense.



Situation Analysis

In this age where data and information are the new currency, Australian organisations of all sizes have a strong awareness of the legal requirements surrounding storing, keeping and disposing of confidential data. However, within the 2015 Security Tracker for Australia, there is a strong trend emerging that suggests many organisations and individuals are not auditing, assessing, reviewing or implementing such policies and procedures. This does not bode well for the overall security for any business' confidential or sensitive information.

The 2015 Security Tracker, which surveyed more than 1,100 large and smaller businesses across Australia, revealed a significant lack of understanding and implementation of information security policies among SMEs compared with larger organisations.

Overall business awareness

While 93 per cent of larger organisations and two-thirds of small and medium-sized enterprises (SMEs) have known protocols for storing and disposing of data, half admit that not all employees are aware of these policies.

The research showed that when it comes to auditing their information security procedures, fewer than half of larger organisations and only just over a quarter of small businesses conduct frequent audits. Of great concern is that one in five smaller businesses in Australia have never audited their organisation's information security procedures.

When it comes to training internal staff on these policies and procedures, 73 per cent of C-Suites and only 29 per cent of small businesses conduct training on a yearly basis.

Who is responsible?

Both C-suites and small businesses agree that if information were to be lost or stolen the greatest impact would be on their credibility as an organisation. They also agree that client or customer information would be the most damaging if stolen.

When it comes to 'who' would steal confidential customer or company information, small business owners are much less concerned, 27 per cent, about the possibility that it would be their employees, compared to 69 per cent of C-suites.

This level of trust is also displayed with external suppliers. Half of small businesses surveyed do not vet suppliers for their security protocols, while 90 per cent of C-suites do perform security checks on third-party vendors.

Improving information security

The Australian government's response or commitment to information security is viewed as being excellent by one-third of C-suite executives, however only 12 per cent of small business owners agree. If additional legislation or regulation requiring document destruction were to be introduced by the Australian Government, 38 per cent of small business owners say they do not know what impact this would have on current policies.

The Security Tracker results demonstrate the apparent need for more education and resources, to assist small businesses across Australia with their information security. The survey has highlighted there are still gaps among Australian organisations of all sizes.

BEING AWARE OF THE IMPORTANCE OF INFORMATION SECURITY ISN'T ENOUGH ANYMORE

MOST **LARGE** AND **SMALL BUSINESSES** IN AUSTRALIA
(97%) (83%)
ARE SOMEWHAT AWARE OF THE LEGAL REQUIREMENTS
REGARDING STORING, KEEPING, OR DISPOSING
OF CONFIDENTIAL INFORMATION.



HOWEVER



Only **50%** of large businesses and **45%** of **SMEs** have a **protocol for disposing confidential information** that exists and is adhered to by all employees.



73% of large businesses **train their staff** on their organisation's **security policies** at least once a year, only **29%** of **SMEs** do.



47% of large businesses **audit their information security policies/procedures** whereas only **28%** of **SMEs** do.



80% of large businesses have a **cyber-security policy** but only **40%** of **SMEs** do.



64% of large businesses have a **locked container** in their offices for **disposing of documents** but only **37%** of **SMEs** do.

WITH



\$144AUD

THE AVERAGE COST OF A LOST OR STOLEN RECORD

AND

\$2.820.000AUD

TOTAL AVERAGE COST OF A BREACH

AUSTRALIAN BUSINESSES - NO MATTER WHAT THEIR SIZE - NEED TO CONTINUE
TO IMPROVE AND ENFORCE THEIR SECURITY POLICIES AND PROCEDURES
TO PROTECT THEIR CONFIDENTIAL INFORMATION.



Making sure
it's secure.™

Contact Shred-it to book your free Data Security Survey.
Call 1800 012 012 or visit shredit.com.au.

Hot Topic in Information Security: Operating Securely in a Mobile, Outsourced World

Technology has empowered workers and business owners not only to flexibly work on the go, but also to more readily engage specialist skills through an increasingly outsourced world. The Australian Communications and Media Authority commissioned a study in 2013 that showed 5.6 million people, or 51 per cent of employed Australians, worked some part of their time away from the office. Eight in ten of these mobile workers said home was the main place of work outside of the office; and 22 per cent said they worked away from the office for more than four days in a week. The Authority said it expected these numbers to continue to increase with the proliferation of smart devices and enhanced connectivity.

Although advancements in technology such as the use of laptops and tablets have made it easier for employees to work off-site, these devices pose a greater threat to security than most companies and employees realise. While there is an uptake in workers using electronic devices when working offsite, businesses must not forget that paper documents still pose a hazard to offsite data security. The best way to prevent paper documents from being misplaced is for employees to think twice before removing sensitive documents from the workplace. A robust information security policy that takes into consideration mobile working practices will help employees to understand the risks posed by removing unnecessary confidential documents from the office.

Without proper encryption and firewalls in place on devices and a thorough understanding of company document destruction policies, employees working

outside of the office could be leaving their organisation at greater risk of a security breach. The 2015 Shred-it Security Tracker found that 38 per cent of C-Suite executives have a protocol in place for employees working off site or working from home, with 32 per cent of SMEs also having a similar protocol in place for flexible working. However, more worryingly 35 per cent of SMEs admit they have no policy in place for protecting and disposing of confidential information outside the workplace. By comparison, only 11 per cent of C-Suite executives said they have no off-site working policies in place, showing that large organisations are recognising the importance of extending information security protocols outside the workplace in order to prevent the risk of a data security breach.

There are a number of tips that businesses can follow in order to ensure they work off-site securely. The first step is establishing and implementing a comprehensive training program for employees so that everyone knows exactly how they should treat sensitive and confidential information, both when working in and away from the workplace.

The second is being very clear about what an employee can do when working away from the office. Perhaps it is a no-print, no removal of printed materials, shred-all and definitely no placing materials in standard waste or recycling bins.

Look beyond your own workforce to those of your contractors

In the age of outsourced models where smart businesses engage specialist skills as they require them, organisations should extend their security protocols to all third party suppliers. Any potential suppliers should be vetted on what protocols they have in place and be asked to follow the employing organisations' protocols if they are more stringent.

In particular, this becomes even more crucial when you factor in that many of these specialist contractors are mobile workers in their own right – that is they are working away from their own workplace and often away from your workplace.

It is not out of the ordinary for third party suppliers to attend training or review and sign agreements covering rules of engagement for how to work with an organisation. In manufacturing environments, contractor management is part and parcel of being allowed on site. To extend or put in place a contractor management agreement for third party mobile workers that are focused on the treatment of sensitive and confidential information is essential in today's world.

Getting Started

Businesses have a responsibility to clients to safeguard their sensitive information. Providing comprehensive training and guidelines for employees and third party suppliers to follow when working away from the workplace is a simple measure for companies to bolster their information security. In this competitive environment it's crucial for businesses' survival that they take every step possible to protect their assets. It's also key to recognise and respond to the changing legal landscape when it comes to managing an increasingly mobile and contracted workforce.

Some tips to help:

- Assume all business documents are confidential – and should be removed from the office only if necessary.
- Bring all confidential documents back to the office to be securely disposed of and shredded by a reputable data destruction provider.
- Implement a clean-desk policy at home: lock away confidential documents and work devices when not in use.
- Avoid printing confidential information from laptops or other computers.

Best Practice Tips: Reduce, Remove, Replace

Reduce the need to decide what is confidential

Remove Recycling Bins

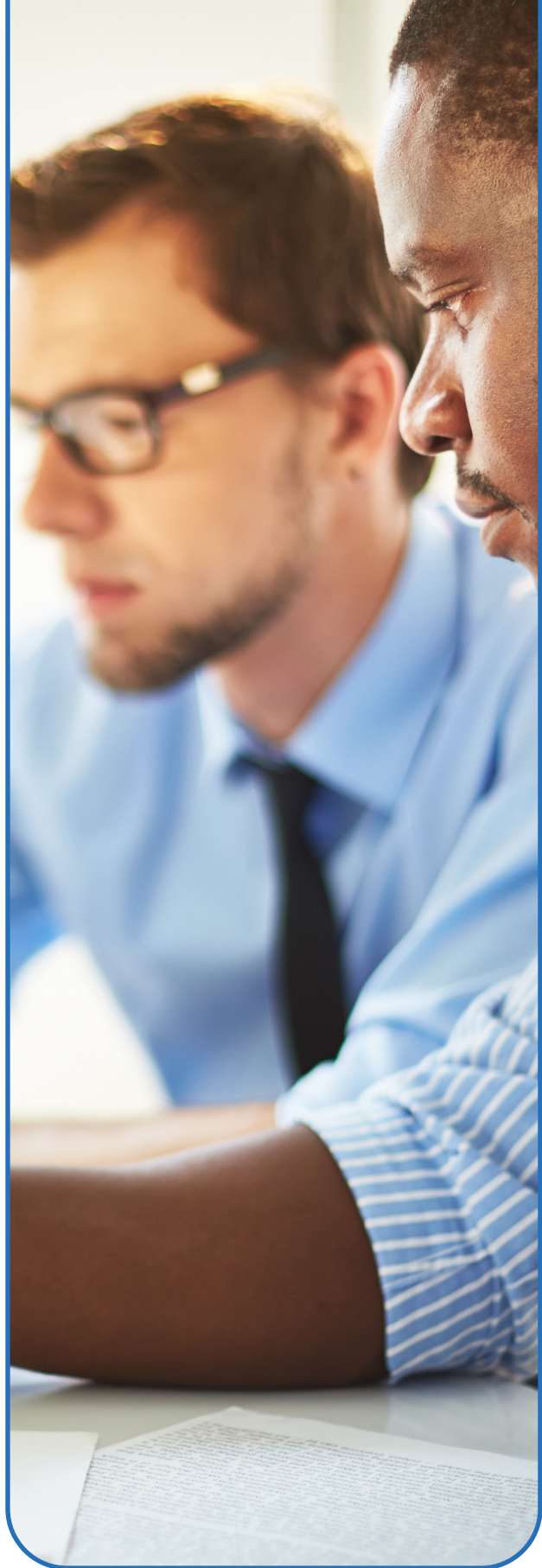
Replace with Secure Destruction Containers

There's an age old saying that you should never air your dirty laundry in public. And most people tend to follow this as best possible in our private lives. Yet in the workplace, where open environments are more the norm than private locked office spaces, waste and recycling bins have the potential to contain just that - professional 'dirty laundry' or confidential information.

Today the most likely source of a security breach doesn't come from a malicious outsider, but rather from within your organisation. According to a recent study, almost 90 percent of respondents said they personally knew a company that had sensitive or confidential data stolen as a result of an insider threat¹ adding considerable urgency to the need to change the way we work.

As data and information becomes the new currency, never before has the need to securely store and destroy confidential data been a higher priority.

Yet Shred-it's 2015 Security Tracker in Australia revealed that only two thirds of Australian SMEs have a known protocol for storing and disposing of confidential data; and more than 80 per cent of all Australian businesses still have waste or recycling bins under people's desks.



1. <http://www.websense.com/assets/reports/report-ponemon-2014-part2-summary-australia-en.pdf>

Remove + Replace = Reduce

One of the easiest ways to reduce the likelihood of an information security breach is to eliminate waste and recycling bins and introduce secure, locked containers for document destruction. By removing the need for employees to determine what is and isn't confidential, you remove an opportunity for human error to creep into your information security practices.

Diarise eWaste Destruction

Once you have your paper-based waste locked down, it is time to consider the plethora of eWaste that is likely sitting around your premise. In its 2015 Security Tracker Shred-it found an astounding 40 per cent of Australian SMEs have never disposed of hard drives, USBs and other hardware containing confidential data.

The best policy is to have on speed-dial the services of a reputable eWaste destruction company; practically companies should look to diarise a regular audit of hardware and arrange for its destruction.

Remember, simply wiping hard drives and media is not fool-proof – most data can be restored. Finally, when considering all options, review the chain of custody that your secure destruction service offers. An auditable trail to provide you with confidence of the data's journey through to final destruction is the best approach.

Top tips for improving information security:

- Demonstrate a top-down commitment from management to the total security of your business and customer information.
- Establish a formal information security policy; train employees regularly to know the policies well and follow them rigorously.
- Conduct periodic security audits. If you don't have the resources to implement a secure document destruction program, work with a reliable third-party vendor.
- Identify security loopholes at every stage of the information cycle, from data generation and storage to the transfer of data from location to location, and eventually to document destruction.
- Introduce a "shred-all" policy, where all waste paper documents are securely destroyed on a regular basis.
- Book in regular audits and destruction of eWaste to minimise valuable data lying around the workplace.
- When working remotely, limit the number of documents you print and try to work primarily on properly encrypted, secure electronic files.
- If you don't have access to a secure shredding source, take your documents with you instead of throwing them in an unsecure recycling bin.
- Never leave unencrypted electronic devices in public places.

Destroy all documents and hard drives using a third-party provider who has a secure chain of custody and confirms destruction.

Asking the Experts

Paul Wallbank, a journalist, reporter and presenter with a focus on small-mid-sized organisations, discusses the importance of reputation to businesses and the damaging effects a data breach can cause. He also explores the need for both large and small businesses to keep confidential information secure and provides top tips for organisations to follow in order to ensure businesses adhere to Australian privacy legislation and do not put themselves at risk of a data breach.

Paul Wallbank: Journalist, Reporter and Presenter

What are some of the challenges being faced by businesses when it comes to maintaining a good reputation?

There are a number of challenges facing businesses today in how they collect and store data; I would suggest customer trust is the issue of crucial importance. We recently saw one example in the US with Target breaching consumer trust; and the Ashley Madison mishandling of consumer information will probably be a defining moment in how consumers treat confidential data online. Customers are becoming increasingly suspicious and wary of the risks associated with data breaches, particularly if their information reaches the public domain.

This area of identity theft and fraud is fast becoming a major issue for all businesses. It doesn't matter if information is stored on paper or digitally, businesses need to demonstrate that they care about their customers and their personal information.

My advice for businesses is to only store what you need - convert big data to small data. For example, if you only need a customer's email address, just store this; you don't need mobile numbers, address details, birthday, or number of children.

By reducing the amount of data that you collect and store, you reduce your risks while increasing your flexibility. If businesses adopt these practices, it will provide a competitive advantage as it demonstrates you care about your customers' information.

How can businesses in Australia suffer if they do damage to their reputations?

A new Privacy Act was implemented in Australia last year. There haven't been any prosecutions yet but when a company is prosecuted under the new law, it will cause major damage to the reputation of the business. The first prosecuted breach will be a major issue and will attract widespread media attention.

In relation to the Privacy Act, there are some other risks associated with information being processed off shore. For instance, there could be a breach of Australian customer information that occurs in India, the US or even Europe via an outsourcing partner of a local business. This highlights the risk of using an outsourcing company and the potential damage which can be caused to organisations who place their trust in them to handle confidential customer information.

This demonstrates that it is not only critical to store information securely, but also to manage the lifecycle of that information from collection to disposal.

What are the specific challenges that small businesses face compared to larger businesses when it comes to protecting confidential information?

Small businesses don't have the necessary resources to help manage the lifecycle of data. Large organisations have dedicated IT staff, teams that are trained in the Privacy Act, software packages and outsourcing contacts, whereas small businesses need to rely on the trust they have with their outsourced partners to do the right thing by them.

The other major risk for small businesses is financial. If a small business experiences a data breach, the impact will be significant. The consequence could be a million dollar hit to their bottom line; this could be detrimental to the point of pushing them out of business. Compare this to a larger business, which would suffer from a damaged reputation; however, they would most likely be able to cope with the financial punishment.

Another major risk for small businesses lies in credit card regulations, the PCI-DSS standards. In some instances small businesses retain data gained through customer credit card use. If the business is found to be holding unauthorised information, the credit merchants will

withdraw their facilities prompting the demise of the small business.

How can larger businesses support smaller businesses in their efforts to keep confidential information safe?

There is a mutual benefit for large and small businesses to keep confidential information safe. If we consider a typical business-to-business relationship, many larger businesses are at risk if their smaller business partners breach confidentiality. For example, if a small suburban computer shop breached the credit card security policy, not only would the reputation of the small business be damaged, but also the credit card merchant.

Supply chain and logistics are crucial to ensure data is not breached. Whoever is the weakest link can cause a domino effect for the entire supply chain. Again let's consider a typical example of where a large business' reputation could be damaged by the actions of a smaller contractor: The customer orders his groceries from a major supermarket online and requests the order to be delivered after 6pm on Monday. This information is passed to the outsourced contractor, who now knows the time when the consumer is not at home. A breach of this trust would typically result in the major retailer being blamed and not the delivery driver.

For this reason, it is important for both small and large businesses to work together when it comes to confidential information.

What Government advice is available to help businesses in Australia protect their reputation?

At the moment, State and Federal Governments have some useful guidelines that can help Australian businesses in protecting their reputation; however, they don't have a strong understanding of the challenges that are facing Australian businesses. It is up to the private sector vendors to step up and take a lead on this. Government agencies are two years behind the information security industry, as it is changing and evolving so rapidly.

My advice for businesses starting out in the industry today is that they should only collect the data you need. In an age of big data, this is only going to overwhelm you. In addition, keep all information secure and comply with all regulations.

Recent Changes in Privacy Legislation

As personal information becomes increasingly vulnerable to security breaches, information security and protection is a top priority for individuals, organisations and governments. Privacy laws and regulations in Australia are constantly being reviewed and updated to ensure they stay up-to-date with technology and the ever-changing nature of the information security industry. In this section, we dive into the key privacy laws and regulations that are applied to government agencies and private sector organisations in Australia.

The Privacy Act 1988

The Privacy Act 1988 is a law in Australia that regulates the handling of individual's personal information from the point of collection through to disposal. Examples of personal information include the name, address, date of birth, bank account details and specific characteristics and opinions of an individual.

The Privacy Act was passed in 1988 and came into force in 1989 under the Office of the Australian Information Commissioner (OAIC). Major reforms to this Act came into play in March 2014, including the development of 13 Australian Privacy Principles (APPs). These apply to the management and use of personal information by APP entities, which are defined as:

- Australian and Norfolk Island Government agencies;
- Private sector organisations with an annual turnover of \$3 million or more that are conducting business in, or collecting information from, individuals in Australia; and,
- A small business or individual that provides health services or holds any health related information (except in an employee record).



The Privacy Act also covers the following:

- The handling of tax file numbers;
- The management of sensitive information such as personal health records;
- Approval and registration of enforceable APP codes that have been developed by an APP code developer, or developed by the OAIC;
- Small business operators that request to be covered by the APPs and any relevant APP code;
- The development of new privacy regulations.

The Australian Privacy Principles

The APPs replaced the Information Privacy Principles (IPPs), which applied to Australian and Norfolk Island Government agencies, and the National Privacy Principles (NPPs), which applied to private sector organisations.

The APPs are a set of legal principles that form the basis of the Privacy Act. The APPs provide an outline of standards and obligations for APP entities in relation to the handling and use of personal information. Despite being a clear set of principles, they can also be flexible, so that handling practices of personal information can be tailored to meet specific needs and business models.

The APPs aim to reflect the lifecycle of handling personal information to ensure transparency from collection through to disposal. Importantly, the APPs equally apply to paper-based and digital forms of handling personal information.

The 13 APPs are categorised into five key parts, outlined below:

Part 1: Consideration of personal information privacy

- APP 1: open and transparent management of personal information
- APP 2: anonymity and pseudonymity

Part 2: Collection of personal information

- APP 3: collection of solicited personal information
- APP 4: dealing with unsolicited personal information
- APP 5: notification of the collection of personal information

Part 3: Dealing with personal information

- APP 6: use or disclosure of personal information
- APP 7: direct marketing
- APP 8: cross-border disclosure of personal information
- APP 9: adoption, use or disclosure of government related identifiers

Part 4: Integrity of personal information

- APP 10: quality of personal information
- APP 11: security of personal information

Part 5: Access to, and correction of, personal information

- APP 12: access to personal information
- APP 13: Correction of personal information.

The OAIC also provides a set of APP guidelines. These guidelines outline necessary requirements, examples of how to apply APPs in different environments and how to adopt good privacy practices.

The APPs and guidelines should be an important component of the staff induction process for any business. It is comforting to know that the 2015 Security Tracker found 97 per cent of C-suite executives were aware of legal requirements relating to personal information, as were 83 per cent of small business owners.

Other significant changes to the Privacy Act

Beyond the APPs, other key changes that Australian organisations need to comply with, and that have an impact on the storage and destruction of sensitive data include:

- New credit reporting provisions;
- A new requirement for a credit provider to be a member of the External Dispute Recognition scheme (EDR scheme);
- New laws on codes of practice about information privacy (APP codes) and a code of practice for credit reporting (the CR code);
- New enforcement powers for the OAIC which include:
 - Assessments of privacy compliance for Australian Government agencies and some private sector organisations;
 - Accepting enforceable undertakings;
 - Seeking civil penalties when serious or repeated breaches of privacy are found.

The 2015 Security Tracker revealed that only 46 per cent of C-suite executives and 21 per cent of small business owners believed they would have to change their information security policies if new privacy legislation was introduced. This is a significant finding, which highlights the importance of staff training and regular audits of company policies.

How to comply with the Privacy Act

To ensure APP entities fully comply with the Privacy Act, all personal information should be managed in a secure and lawful manner. Responsible steps must be taken to:

- Protect information from misuse, fabrication, loss or damage; and
- Destroy information once it is no longer required or securely retain information to meet other legal obligations.

If responsible steps are not taken, individuals and organisations are at risk of breaching the Privacy Act and could be subject to civil penalties. For example, a serious or repeated breach of privacy could attract a maximum penalty of \$340,000 for an individual or \$1.7 million for an organisation.

Interestingly, the 2015 Security Tracker found that 59 per cent of small business owners didn't believe they would face a penalty if personal information was lost. On the contrary, 76 per cent of C-suite executives were aware that this would breach the Privacy Act and would incur a penalty.

Some simple tips on how to best comply with the Privacy Act are as follows:

- Use passwords to restrict access;
- Educate and train staff on the APPs and APP guidelines;
- Monitor and regularly update facilities to ensure maximum security;
- Ensure the proper disposal of all paper-based and digital forms of personal information.

Summary

The results of the inaugural Australian Security Tracker by Shred-it have revealed there is a requirement for more education and awareness for organisations of all sizes when it comes to information security. Particular focus should be applied to Australian Small and Medium Sized Businesses to assist in preventing potentially damaging data security breaches.

Privacy laws and regulations are regularly being reviewed and updated to reflect the current state of the information security industry and keep up with technology. It is therefore crucial to find a balance between information security awareness for the current practices that are in place and being ready for what is to come in the near future.

The first step to data security is being aware of the dangers and the consequences of a data breach. To prevent a security threat it is important to implement policies to protect employees, customers and the business itself from the possible impact of a breach. Following some simple best practices will ensure the business is safe and securely stores and destroys confidential information.

As the data security landscape continues to evolve, businesses must stay ahead if they are to ensure they remain protected and keep reputations intact.

For more tips on improving information security, please visit the Shred-it Resource Centre at shredit.com.au/resource-centre

