Complying with Australian Privacy Law: *Protecting Privacy with Endpoint Security*

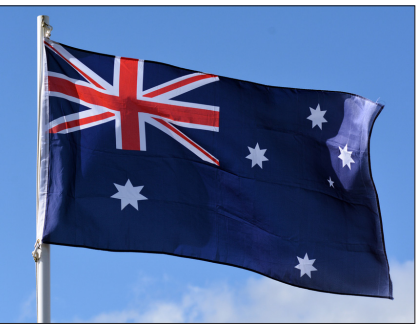


Table of Contents

Business and security professionals recognize the risks: 72% say their top mobile security concern is data loss due to lost or stolen devices.

Highlights:

- Lost or stolen devices increase the risks of unauthorised disclosures of sensitive information
- Business and security professionals recognize the risks: 72% say their top mobile security concern is data loss due to lost or stolen devices
- The rate of mobile device theft is higher than ever: 25% of companies experienced a theft in 2014
- Data on the devices can be attractive targets for thieves: credit card records go for $15 apiece in Australia and in some countries, complete healthcare patient dossiers fetch up to $500
- Research shows Australian organisations are bearing significant costs from data breaches, with almost half of breaches studied due to lost or stolen devices
- Overall costs for a single breach in Australia range from approximately $850,000 to $8.5 million
- Under the recently updated privacy law, Australian organisations have heightened responsibilities to protect personal information, including data residing on endpoint devices
- Non-compliant organisations face penalties and increased enforcement
- Revisions to the privacy law include 13 Australian Privacy Principles (APPs) that regulate the handling of personal information effective as of March 2014
- *APP11 – Security of Personal Information* requires organisations to take **reasonable steps** to protect information
- Reasonable steps are defined in the Australian government's guides to information security and data breach notification, including a range of appropriate safeguards and steps to take in response to a data breach
- Key requirements related to endpoint security can be derived from the guidance documents as well as the ISO/IEC 27002 standard
- Organisations are required to protect computer hardware (including devices) as well as the data (including personal information) that the computer hardware holds from misuse, interference, loss, unauthorised access, modification, and disclosure
- In the case of a missing device, organisations should be able to determine facts such as what data is on the device, whether it has been lost or stolen, where it is, who is in possession of the device, the status of encryption, and if any personal information was accessed by unauthorised users
- Absolute's persistence technology helps organisations to successfully meet the key requirements related to endpoint security and to mitigate the risks of a data breach involving missing devices
- With Absolute persistence technology in place, organisations can:
  - Significantly reduce the chances of devices being lost or stolen
  - Effectively implement risk management and governance strategies for corporate assets
  - Capably handle events involving missing devices
  - Ensure the security of the device and protection of information

Endpoint Devices: Increasing Risks for Organisations

With a growing number and wider array of endpoint devices being used by employees – from laptops and notebooks to tablets and smart phones – more and more devices contain sensitive information such as customer credit card numbers, consumer biographical data or patient health records.

Chief Information Security Officers (CISOs) today are well aware that the proliferation of endpoint devices is creating major risks. Organisations continue to enable an increasingly mobile workforce. A government study on the "digital worker" found that over half of Australia's workers were using Internet-connected devices to work away from the office.[1] In some industries, the use of mobile devices for work is extensive. For example, research indicates 87% of healthcare professionals use a mobile phone in clinical practice.[2]

In fact, many Australian organisations were early adopters in deploying mobile devices to employees and supporting Bring Your Own Device (BYOD).[3] With a growing number and wider array of endpoint devices being used by employees — from laptops and notebooks to tablets and smart phones — more and more devices contain sensitive information such as customer credit card numbers, consumer biographical data or patient health records.

THE POTENTIAL FOR UNAUTHORISED DISCLOSURES

As some endpoint devices inevitably go astray, organisations face the potential for unauthorised disclosures of personal information. In a recent survey of business and security professionals, 72% say their top mobile security concern is data loss due to lost or stolen devices.[4] It turns out, they have real cause for concern. Worldwide, the rate of mobile device theft has continued to climb over the years, with 25% of companies experiencing a theft of a mobile device in 2014, a significant increase from the 14% reported in 2011.[5]

The motivation to steal endpoint devices is on the rise given the black market value of personal data like credit card numbers and health records. Nowadays perpetrators can expect to profit not only from reselling the hardware but also peddling the data. The average market price for a credit card record in Australia is $15.[6] Other personal data can be even more valuable; for example a study in the U.S. found that health records can sell for $20 and complete patient dossiers for $500.[7]

INCREASING OBLIGATIONS TO PROTECT INFORMATION

Safeguarding endpoint devices poses enormous challenges, given the volume and variety of devices and lack of control over end-user behaviour. Yet under the recently updated privacy law in Australia, there are heightened responsibilities for organisations to protect personal information, including data residing on endpoint devices. Non-compliant organisations face penalties and increased enforcement.

THE RISING COSTS OF DATA BREACHES

According to the *2014 Cost of a Data Breach Study: Australia*,[8] organisations in Australia continue to suffer data breaches due to lost or stolen devices and are bearing significant costs. Of the data breaches examined in the study, 45% involved lost or stolen devices. The study also revealed that a lost or stolen device was the number one factor in increasing the cost of a data breach. Overall costs for a single breach ranged from approximately $850,000 to $8.5 million. Costs included detection and escalation activities, meeting notification and regulatory requirements, remediation and legal expenditures; and lost business. In fact, more customers are now abandoning companies following a data breach; the costs due to lost business have reached a new high.

THE IMPORTANCE OF ENDPOINT SECURITY

Endpoint security plays a key role in developing effective strategies to protect information, comply with the updated privacy law, and mitigate the risks and costs of data breaches. Specifically, a persistent security and management solution for endpoint devices provides organisations with a trusted lifeline to all devices, and arms them with a range of powerful capabilities to remotely control and monitor devices and protect the information they contain. This white paper outlines the general requirements of the updated privacy law and associated guidance, and the specific requirements pertaining to endpoint security. It details how Absolute's patented persistence technology assists organisations in meeting the requirements related to endpoint security, including helping to prevent devices from getting lost or stolen and to limit the damage when incidents occur.

The New Law: Getting Serious About Privacy

Recent revisions to the Privacy Act (1988)[9] show the Australian government is determined to ensure that organisations that hold personal information take their responsibilities seriously. The amendments include 13 Australian Privacy Principles (APPs) that regulate the handling of personal information effective as of March 2014.[10]

Australian Privacy Principles

APP 1 – Open and transparent management of personal information
APP 2 – Anonymity and pseudonymity
APP 3 – Collection of solicited personal information
APP 4 – Dealing with unsolicited personal information
APP 5 – Notification of the collection of 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
APP 10 – Quality of personal information
APP 11 – Security of personal information
APP 12 – Access to personal information
APP 13 – Correction of personal information

WHAT HAS CHANGED?

- The regulator's enforcement powers have been increased including the ability to levy higher penalties and impose enforceable undertakings against non-compliant organisations.
- Significant modifications to the principles regarding the use and disclosure of personal information for direct marketing purposes and cross-border disclosures of personal information.
- Expanded requirements and updated guidance related to the security of personal information and data breach notification.

WHO IS COVERED?

- Organisations having responsibilities under the Privacy Act generally include:
  - Australian Government agencies
  - Businesses and not-for-profit organisations with an annual turnover more than $3 million
  - Specific types of small business operators with an annual turnover of $3 million or less such as private sector health service providers, businesses that sell or purchase personal information, and credit reporting bodies

WHAT DATA MUST BE PROTECTED?

- The Privacy Act defines personal information broadly as *"...information or an opinion, whether true or not, and whether recorded in a material form or not, about an identified individual, or an individual who is reasonably identifiable."*
- Common examples are an individual's name, signature, address, telephone number, date of birth, medical records, biometric information, bank account details, photos, memberships, place of work, and opinions.

Security Requirements: Taking Reasonable Steps to Protect Information

The Australian Privacy Principles (APPs) include *APP11 – Security of Personal Information.* APP 11 contains the general requirement for organisations to take **reasonable steps** to protect information (see sidebar). But what are reasonable steps?

The Australian government provides guidance on the reasonable steps that entities are required to take under the Privacy Act in their *Guide to information security: 'Reasonable steps' to protect personal information*. The guide was recently revised and brought in line with the updated Privacy Act, including the APPs. The *Consultation draft: Revised Guide to information security* was released in August of 2014.[11]

APP 11 – Security of Personal Information

APP 11.1 states that "If an APP entity holds personal information, the entity must take such steps as are reasonable in the circumstances to protect the information:
(a) from misuse, interference and loss; and (b) from unauthorised access, modification or disclosure."

APPROPRIATE SECURITY SAFEGUARDS

"Reasonable steps" depend on circumstances such as the nature of the entity (i.e. size, resources and business model) and amount and sensitivity of the personal information held by the entity, etc. Entities are advised to undertake an information security risk assessment to determine appropriate safeguards and review them on an ongoing basis. The guide outlines a range of appropriate safeguards, including strategies for:

- Managing information lifecycle
- Governance
- Information and communications technology (ICT) security
- Access security
- Data breaches
- Physical security
- Personnel security and training
- Destruction and de-identification
- Internal practices, procedures, and systems
- Standards

For the use of standards, the guide specifically recommends the ISO/IEC 27000 information security management systems standards. Entities are encouraged to adopt standards as a way to gain some confidence regarding their security practices and ensure they are taking reasonable steps to protect personal information.

Data Breach Notification: Applying a Risk-Based Approach

For Australian organisations, an increasingly important "reasonable step" in protecting information is to develop and implement a data breach policy and response plan that includes notification. The Australian government has laid out their expectations for organisations in their *Data breach notification guide: A guide to handling personal information security breaches*.[12] An updated guide was released in August 2014 to take account of amendments to the Privacy Act.

The guide states that in general, if there is a **real risk of serious harm** as a result of a data breach, the affected individuals and the Privacy Commissioner should be notified. It stresses the importance of notification in order to mitigate the risks for the affected individuals. If individuals are notified, they may be able to take actions to avert for example, identity theft, financial loss, or damage to their reputation, and so on.

TRANSPARENCY AND TRUST

Organisations are advised that notification of a data breach supports good privacy practice and can promote transparency and trust in their organisation. Although a mandatory obligation to notify has not yet been put into place in Australia (see sidebar); organisations are strongly encouraged to take the steps and actions as outlined in the guide. Another important consideration is that other jurisdictions worldwide are enforcing mandatory breach notification laws.

According to the guide, organisations should be prepared to deal with data breaches that can occur due to many types of incidents, for example:

- Lost or stolen laptops containing personal information
- Hard disk drives being disposed of without the contents first being erased
- Customer databases being 'hacked' into or otherwise illegally accessed

TO NOTIFY OR NOT TO NOTIFY?

In responding to a data breach, a key challenge is determining if and when notification is an appropriate response. The guide encourages a risk-analysis approach. Organisations should look at data breaches on a case-by-case basis and make decisions on actions to take according to their own risk assessment.

The Status of Data Breach Notification

Several years ago, the Australian Law Reform Commission (ALRC) recommended the Privacy Act be amended to include a mandatory obligation for entities to notify the Privacy Commissioner and affected individuals in the event of a data breach. Although the Privacy Act was not amended to include mandatory breach notification, there continues to be on-going debate on the issue. In fact, it was raised again in the Senate in November 2014.

Currently in Australia there is mandatory breach notification in the healthcare sector. Under the Personally Controlled Electronic Health Record Act 2012 (PCEHR), there is compulsory data breach notification for breaches involving PCEHR data.

The Australian government may yet impose mandatory data breach notification at a federal level in the future. In the meantime, organisations can turn to the data breach notification guide. As well, all organisations involved in global commerce must contend with a growing number of mandatory data breach notification requirements in North America, Europe and Asia.

Requirements Pertaining to Endpoint Security

Organisations in Australia face significant risks that an endpoint device with personal information on it will go missing. Therefore it is understandable that the government's *Guide to information security* contains a range of requirements related to endpoint security. It warns that:

> *"...failure by the entity to take reasonable steps under APP 11 to prevent unauthorised access such as a cyber-attack or a* ***theft****...may be a breach of APP 11."*

Key requirements can be derived from guidance documents as well as the ISO/IEC 27002 standard.

PROTECT THE DEVICE AND THE DATA

The guide specifies that under APP 11, entities should implement information security controls that guard against loss or theft of computer equipment or devices containing personal information — including accidental or inadvertent loss. Entities are advised that effective security requires protecting computer hardware (the physical devices that make up a computer system) as well as the data (including personal information) that the computer hardware holds from misuse, interference, loss, unauthorised access, modification, and disclosure.

Requirements for endpoint security are also contained in the ISO/IEC 27000 standards, which entities are encouraged to adopt. The ISO/IEC 27002 standard[13] is an internationally-acclaimed standard of best practice in information security. It is a comprehensive standard with detailed guidance on a broad spectrum of security controls. Controls pertaining to endpoint security include controls regarding:

- Equipment: policy and security measures to prevent loss, damage, theft or compromise of assets
- Mobile devices: policy and security measures to manage the risks introduced by using mobile devices

CONTAIN THE BREACH AND ASSESS THE RISKS

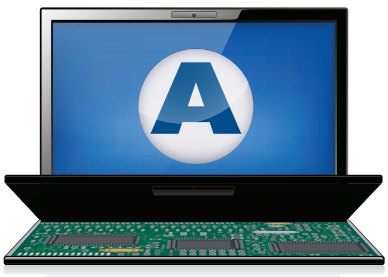
Other requirements pertaining to endpoint security can be found in the *Data breach notification guide*. Organisations are advised to take whatever steps possible to immediately contain the breach. For example, stop the unauthorised practice, recover the records, or shut down the system that was breached. For assessing the risks in the case of a lost or stolen endpoint device, it is particularly difficult to gather the facts needed to decide if a breach of personal information has occurred and if notification is necessary, given that the endpoint device is no longer under the organisation's physical control. To capably manage incidents, organisations should be able to determine things such as what data is on the device, if the device has been either lost or stolen, where the device is, who is in possession of the device, the status of encryption, and if any personal information was accessed by unauthorised users.

For a detailed list of specific requirements related to endpoint security see appendix on page 10.

Meeting the Requirements with Absolute Technology

Absolute's persistence technology helps organisations to successfully meet the key requirements pertaining to endpoint security derived from the updated Privacy Act and associated guidance. As well, Absolute's solution helps to mitigate the risks of a data breach involving missing devices. With Absolute persistence technology in place, organisations can:

- **Significantly reduce the chances of devices being lost or stolen:**
  - Control and secure the complete range of devices in today's IT environment such as servers, workstations, desktops, laptops, notebooks, tablets, and smartphones
  - Track the physical location of devices using geolocation
  - Build geofences whereby administrators are alerted when the device strays out of bounds
  - Monitor suspicious devices to pre-emptively respond to security incidents
- **Effectively implement risk management and governance strategies for corporate assets:**
  - Retain a connection to all devices, on or off the network
  - Run reports on device status to prove that device location, hardware configuration, installed software programs, encryption and security software, etc. are in compliance with policy
  - Know with certainty what is on the device and whether it is secure
  - Remotely delete sensitive information from devices at end-of-life
  - Produce an audit record or end-of-life certificate to prove data was deleted
  - Create customized alerts that indicate if unauthorised changes to the device have been made, or in cases of anomalous device behaviour
  - Track device location history and chain of custody
  - Identify devices that might be at risk
- **Capably handle events involving missing devices:**
  - Protect the personal information on the device by remotely preventing access to the device
  - Freeze the device so that it becomes unusable and send a message to the user
  - Remotely retrieve or delete personal information from the device
  - Detect whether the device is adequately encrypted
  - Determine if sensitive information on the device has been viewed
  - Perform remote forensic investigations to understand how and why a device was breached
  - Obtain detailed information on the device such as IP address and call history
  - Work with law enforcement to recover the device and/or possibly identify and charge the individuals associated with the event
- **Ensure the security of the device and protection of information:**
  - Augment safeguards such as encryption and passwords which can easily be thwarted
  - Protect the organisation from risky end-user behaviours such as posting their password on the device, sharing their password, lending or giving corporate equipment to unauthorised users, or leaving their device unattended in public and susceptible to theft or tampering
  - Add a layer of defence to encryption programs that are vulnerable to a variety of attacks including human error



Patented Absolute Persistence Technology

Absolute technology works because it is persistent and provides the organisation with a trusted lifeline to each device, regardless of user and location. This is possible because the Absolute persistence module is embedded into the firmware of computer, tablet, and smartphone devices at the factory. It is built to detect if the software agent has been removed. If the agent is missing, the persistence module will ensure it automatically reinstalls even if the firmware is flashed, the device is re-imaged, the hard drive is replaced, or if a tablet or smartphone is wiped clean to factory settings.

Conclusion

To meet the security requirements of the Australian privacy law, organisations should take a risk-based approach to determine reasonable steps to protect personal information. Given the risks associated with endpoint devices, endpoint security is a key aspect of an effective information security strategy, specifically persistence technology which provides a trusted lifeline to all devices.

The benefits of implementing Absolute's persistent security and management solution go beyond compliance. With Absolute's solution, organisations can mitigate the risks of data breaches, enabling them to safeguard their reputation and avoid significant costs. As well, organisations can protect not only devices that hold personal information but also devices that contain other types of sensitive data such as intellectual property and financial records.

With Absolute's solution, organisations can mitigate the risks of data breaches, enabling them to safeguard their reputation and avoid significant costs.

Absolute Software: The Trusted Expert in Persistent Security and Management

- Absolute is the industry standard in persistent endpoint security and management solutions for computers, laptops, and smartphones — and the data they contain.
- Absolute Software has been a leader in device security and management for over 20 years.
- Absolute persistence technology is proven technology that is built into tens of millions of devices around the world.
- Absolute enables a variety of forensic functionality to assist the investigation and recovery of stolen computers, or confidential insight into internal criminal activity or corporate non-compliance.
- Absolute Computrace allows administrators to remotely engage with devices, which includes the ability to delete sensitive data or remotely freeze a device that is at risk.
- The Absolute Investigations team has recovered more than 30,000 stolen devices in over 100 countries.

---

[1] Home is where the work is – the digital worker, Australian Communications and Media Authority Blog, October 2013

[2] Healthcare professionals' use of mobile phones and the internet in clinical practice, Journal of Mobile Medicine, April 2013

[3] Australian enterprises more likely to be in 'mobile void, ZDNet, July 2014

[4] 2014 Mobile Security Survey, InformationWeek, March 2014

[5] IT Security Risks Survey 2014, Kaspersky Lab, September 2014

[6] The Cybercriminal's Prize: Your Customer Data and Competitive Advantage, Forrester, August 2014

[7] Brief: Stolen And Lost Devices Are Putting Personal Healthcare Information At Risk, Forrester, September 2014

[8] 2014 Cost of a Data Breach Study: Australia, Ponemon Institute, May 2014.

[9] Privacy law reform, Australian Government Website

[10] Australian Privacy Principles guidelines, Australian Government, revised March 2014

[11] Consultation draft: Revised Guide to information security – 'Reasonable steps' to protect personal information, Australian Government Website

[12] Data breach notification guide: A guide to handling personal information security breaches, Australian Government Website

[13] ISO/IEC 27002:2013 Information technology – Security techniques – Code of practice for information security controls, ISO Website

APPENDIX

Privacy Law Associated Guidance: Key Requirements Related to Endpoint Security

Revised Guide to Information Security: Reasonable Steps to Protect Information
• Guard against loss or theft of computer equipment or devices containing personal information — including accidental or inadvertent loss
• Protect both computer hardware (the physical devices that make up a computer system) as well as the data (including personal information) that the computer hardware holds from misuse, interference, loss, unauthorised access, modification, and disclosure
• Put in place controls to prevent unauthorised access or theft of personal information
• Guard against unauthorised use or disclosure of personal information as a result of human error (for example, the misplacing of hardware components and peripheral devices such as laptops)
• Monitor points of access to personal information (such as devices) to determine anomalous patterns
• Establish clear policies governing the use of portable/mobile devices
• Implement security specifications for personal/mobile devices such as passwords and encryption
• Use relevant standards for information security
ISO/IEC 27002 Standard
• Implement controls (policy and supporting security measures) pertaining to equipment* such as:
◦ Prevent loss, damage, theft or compromise of assets
◦ Ensure all removal of equipment is authorised
◦ Institute time restrictions on the removal of assets and record all removals and returns
◦ Undertake spot checks to detect unauthorised removal
◦ For off-site assets, take into account the different risks of working outside the organisation's premises
◦ Maintain a log which details the chain of custody for the equipment
• Implement controls (policy and supporting security measures) pertaining to mobile devices such as:
◦ Put in place registration of mobile devices
◦ Ensure physical protection of devices
◦ Restrict software installation on devices
◦ Deploy access controls for devices
◦ Protect devices with cryptographic techniques
◦ Have the ability for remote disabling, erasure, or lockout
◦ Protect against the unauthorized access or disclosure of the information stored and processed by devices

* Information storing and processing equipment includes all forms of personal computers, organisers, and mobile phones, etc.

Data Breach Notification Guide: A Guide to Handling Personal information Security Breaches
• Contain the breach
◦ Take whatever steps possible to immediately contain the breach. For example, stop the unauthorised practice, recover the records, or shut down the system that was breached.
• Assess the risks
• In the event of a lost or stolen endpoint device, the organisation should be able to answer such questions as:
◦ What personal information was on the device?
◦ Who may be affected by the disclosure of this personal information?
◦ What parties have gained unauthorised access to the device?
◦ Have they viewed the personal information on the device?
◦ Is there a risk of ongoing breaches or further exposure of the information on the device?
◦ Is there evidence that someone stole the device?
◦ Can it be determined whether the thief specifically wanted the information on the device, or the hardware itself?
◦ Is the personal information adequately encrypted on the device?
◦ Can the device and personal information be recovered?
◦ Who is in possession of the device and the affected information?

NOTE: The information contained in this document on the Privacy Act, APPs, and security requirements is provided as general summary information only. The list of requirements stated is limited to a small subset of the information security requirements — those pertaining to endpoint security. Organisations should refer to the Privacy Act, APPs, and associated guidance publications for comprehensive guidance on complying with the law including the complete set of requirements. Explanations regarding the Absolute technology solution and how it can help organisations to implement security controls for endpoint security are also provided as general summary information only. Organisations must work with legal counsel and/or privacy and information security auditors to determine if their particular implementation of security controls meets the requirements of the law.