Organisational Privacy in the Digital Age

Policies, practices and pitfalls what you need to know

Presented by Katherine Sainty

sainty law

OVERVIEW

Topics we will cover today:

- Privacy
  - Updated Privacy Obligations: Notifiable Data Breach Scheme
- Spam

What You should be doing:

At Sainty Law we are committed to protecting your information.

We recently updated our Privacy Policy to incorporate the Notifiable Data Breach Scheme.

Our updated policy provides more details on:

- the information that we collect;
- how we use this information, why we store, and why we retain it; and
- how you can request that your information is updated, corrected, or deleted.

Privacy

sainty law

PRIVACY

- The *Privacy Act 1988* (Cth) and the Australian Privacy Principles or APPs set out in the Privacy Act regulate the way organisations collect, hold, use, disclose and dispose of information that personally identifies individuals.
- The Office of the Australian Information Commissioner (**OAIC**) is the responsible regulator.
- The maximum penalty for serious and repeated breaches of the Privacy Act is **$2.1 million**.

PRIVACY

personal information

- **Information about** an **individual**, who is reasonably **identifiable**:
  - opinions
  - true or not; and
  - recorded in a material form or not.
- eg a person's name, address, contact information and TFN, IP address

sensitive information

- A subset of personal information that requires **further protection**
- e.g. racial, religious, political information and health information, sexual orientation

PRIVACY

- The APPs are structured to reflect the personal information lifecycle. They are grouped into five parts:
  - Part 1 – Consideration of personal information privacy (APPs 1 and 2)
  - Part 2 – Collection of personal information (APPs 3, 4 and 5)
  - Part 3 – Dealing with personal information (APPs 6, 7, 8 and 9)
  - Part 4 – Integrity of personal information (APPs 10 and 11)
  - Part 5 – Access to, and correction of, personal information (APPs 12 and 13)

Part 1 – Consideration of personal information privacy

Principle	Summary
APP 1: Open and transparent management of personal information	Entities will manage personal information in an open and transparent way. This includes having a clearly expressed and up to date privacy policy.
APP 2: Anonymity and pseudonymity	Entities will give individuals the option of not identifying themselves, or of using a pseudonym. Limited exceptions apply.

Part 2 – Collection of personal information

Principle	Summary
APP 3: Collection of personal and sensitive information	Entities will collect personal information 'reasonably necessary' for one or more of its functions or activities. Higher standards are applied to the collection of 'sensitive' information.
APP 4: Dealing with unsolicited personal information	Entities will assess whether it could have collected unsolicited information under APP 3 and if not, destroy or deidentify that information.
APP 5: Notification of the collection of personal information	As soon as practicable after collection, entities will notify the individual of its identity, how to contact it, the purposes of collection, usual disclosures to third parties, complaint handling process and likely overseas disclosure.

Part 3 – Dealing with personal information

Principle	Summary
APP 6: Use or disclosure of personal information	Entities will only use or disclose personal information that it holds for purpose for which it was collected or secondary purpose if an exception applies.
APP 7: Direct marketing	Entities may only use or disclose personal information for direct marketing purposes if certain conditions are met.
APP 8: Crossborder disclosure of personal information	Entities will take reasonable steps to protect personal information before it is disclosed overseas to ensure the overseas recipient does not breac the APPs. Entities will be accountable for a breach of the APPs by an overseas recipient, subject to some exceptions.
APP 9: Adoption, use or disclosure of government related identifiers	Only under limited circumstances can entities adopt a government related identifier of an individual as its own identifier, or use or disclose a government related identifier of an individual.

Part 4 – Integrity of personal information

Principle	Summary
APP 10: Quality of personal information	Entities must take reasonable steps to ensure the personal information it collects, uses or discloses is accurate, up to date and complete, having regard to the purpose of the use or disclosure.
APP 11: Security of personal information	Entities must take reasonable steps to protect personal information it holds from misuse, interference and loss, and from unauthorised access, modification or disclosure. Entities has obligations to destroy or de-identify personal information in certain circumstances.

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

Principle	Summary
APP 12: Access to personal information	Entities will give access to personal information held about an individual on their request.
APP 13: Correction of personal information	Entities will correct the personal information it holds about individuals to ensure it is accurate, up to date, complete, relevant and not misleading.

Updated Privacy Obligations

sainty law

NOTIFIABLE DATA BREACH SCHEME

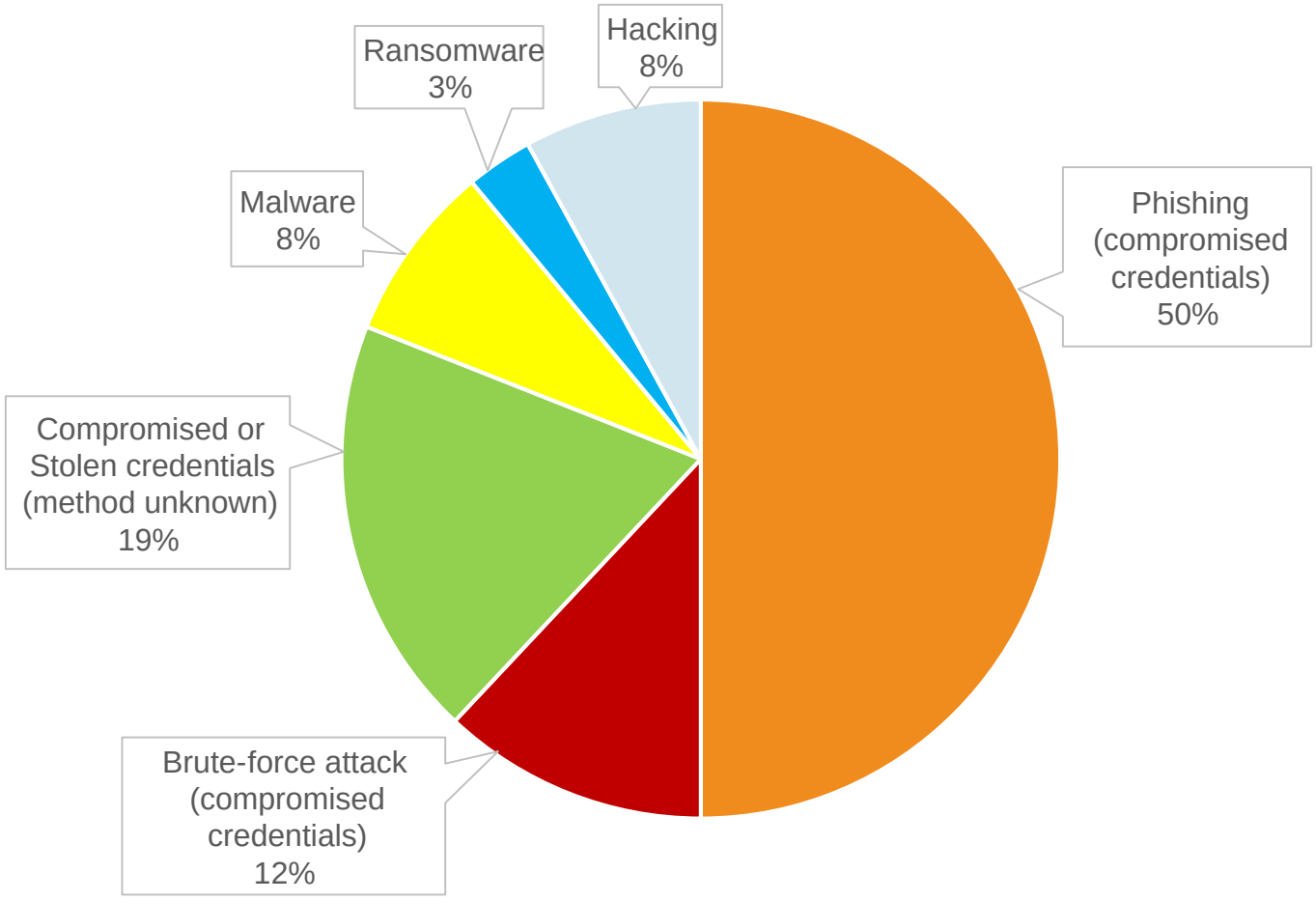
- The Notifiable Data Breach Scheme came into effect 22 February 2018
- Notify OAIC and affected individuals as soon as practicable if you have reasonable grounds to believe that an eligible data breach has occurred
  - **Eligible data breach** where a reasonable person would conclude that an unauthorised access or disclosure of information would be likely to result in **serious** harm to the individual to whom the information relates.
- Balanced assessment to determine if the data breach has notification obligations?
  - **Premature notification** can cause adverse impact eg worse reputational consequences
  - Effective **remediation** strategies instead

WHAT ARE THE TYPES OF CYBER THREATS & NOTIFIABLE DATA BREACHES

Top cyber threats which may impact businesses or cause reportable data breaches:

- Employees or contractors stealing confidential information
- Opportunistic attackers deploying ransom wear
- Business email fraud including phishing
- Advanced attackers hacking your systems

OAIC CYBER INCIDENT BREAKDOWN



EFFECTIVE INCIDENT RESPONSE

contain & remediate

- take all steps to **contain breach** as quickly as possible
- take all steps to **mitigate or remediate any harm** to affected individuals and organisation

risk assessment

- Identify the nature, cause and extent of the breach
- Assess the **level of risk** that the breach creates

EFFECTIVE INCIDENT RESPONSE

notify
(if appropriate)

- notify if legally required
- notify if risk assessment mandates

post breach assessment

- investigate **how and why** breach occurred
- determine preventative measures
- implement new measures

CASE STUDY: INEFFECTIVE CONTAINMENT

- **2013-2016 Yahoo! Data Breach**
- **Yahoo!** (rebranded as Oath) suffered a series of cyber security incidents since 2013 which is now estimated to have affected a 3 billion of its users - **largest recorded data breach** in history
- **Cyber Security Incidents occurred:**
  - **2013 –** 1 billion user account information stolen
  - **2014 –** 500 million user account information stolen
  - **2015-2016 –** 32 million user accounts accessed (Cookie Forging Activity)
- Certain remedial actions: notifying 26 specifically targeted users and significant additional security measures implemented
- Risk Assessment –
  - **Scale of breach:** large
  - **Nature of breach:** personal information
  - **Risk of harm:** high
  - **Business risks:** reputational damage (high), damages (low) , loss of trust and public confidence (high)
- Notification –
  - Yahoo! disclosed the Cyber Security Incidents in 2013 (3 years later)

CASE STUDY: EFFECTIVE CONTAINMENT

- 2014 JP Morgan Chase Data Breach
- Files containing personal information of more than 83 million accounts leaked
- Hackers obtained list of JP Morgan's applications and cross-checked them against known vulnerabilities to identify an entry point
- Contain & remediate: able to identify breach and remove malware before any highly confidential data was stolen
- Risk Assessment –
  - Scale of breach: large
  - Nature of breach: personal information
  - Risk of harm: high
  - Business risks: reputational damage (high), damages (low) , loss of trust and public confidence (high)
- Notification –
  - Notification to all affected parties and formal investigation

CASE STUDY: INEFFECTIVE RISK ASSESSME

- 2017 Equifax Data Breach
- Data containing **personal information** of **more than 145 million** consumers accessed by hackers through flaw in Equifax software
- Equifax aware of security flaw but failed to update the software which resulted in the breach
- Risk Assessment – Waited until it observed "additional suspicious activity" to take action
  - **Scale of breach**: large (5th largest data breach in history)
  - **Nature of breach**: personal information
  - **Risk of harm**: high
  - **Business risks**: reputational damage (high), damages (high), loss of trust and public confidence (high)
- Notification –
  - Late notification (more than a month) to affected individuals

CASE STUDY: INEFFECTIVE RISK ASSESSME

- 2017 Amazing Rentals Pty Ltd Breach
- **Private information** from **4,000 Amazing Rentals' customers** leaked online, including ID documents (drivers licences), financial information, credit application forms, Centrelink records and bank statements.
- The Australian Privacy Commissioner has finalised inquiries into the data breach. **Amazing Rentals has ceased trading and is no longer contactable.**
- Risk Assessment –
  - **Scale of breach**: medium
  - **Nature of breach**: personal information
  - **Affected individuals**: 4,000
  - **Risk of harm**: high
  - **Business risks**: reputational damage (high), damages (high), loss of trust and public confidence (high)
- Notification –
  - OAIC then took steps to prevent the information continuing to be publicly accessible and to notify Amazing Rentals' former customers of the data breach

CASE STUDY: INEFFECTIVE NOTIFICATION

- **2016 Uber Data Breach**
- Data containing **personal information** of **57 million** users was downloaded by hackers from a third-party cloud server also used by Uber
- Risk Assessment –
  - **Scale of breach**: large
  - **Nature of breach**: personal information
  - **Affected individuals**: 57 million
  - **Risk of harm**: high
  - **Business risks**: reputational damage (high), damages (high), loss of trust and public confidence (high)
- Notification –
  - No notification to affected individuals or regulators until a year later, Uber covered up the breach by paying hackers $100,000 **on a promise** to delete the data

CASE STUDY: EFFECTIVE NOTIFICATION

- 2016 Red Cross Data Breach
- File containing **personal information** (incl. **sensitive information**) of **1.28 million** blood donors accidentally placed on an unsecured, public-facing part of website
- Error occurred by a contractor responsible for the management of the Red Cross website
- Risk Assessment –
  - **Scale of breach**: large (Australia's biggest incident)
  - **Nature of breach**: personal information and sensitive information
  - **Affected individuals**: 1.28 million
  - **Risk of harm**: high (sensitive nature of information)
  - **Business risks**: reputational damage (high), damages (high), loss of trust and public confidence (high)
- Notification –
  - Notification to all affected parties and formal investigation

Spam

sainty law

SPAM

- *Spam Act 2003* (Cth) regulates sending commercial electronic messages (CEMs). The Australian Communications and Media Authority is the responsible regulator.
- A CEM is any electronic message (email, SMS, MMS, instant messaging) which, having regard to all the circumstances, has a commercial purpose, i.e. where the message contains an offer to sell, or advertise or promote goods or services
- Under the Spam Act, an organisation may not send CEMs unless:
  - the recipient has given **express or implied consent**
  - the message **identifies the sender** of the message; and
  - the message contains a **functional unsubscribe mechanism.**
- Maximum penalty for two or more contraventions of the Spam is **$2.1 million.**

SPAM: CONSENT

- Recipients must give express **consent (eg** ticking a box on a website) to receive a CEM.
- An organisation cannot send a CEM to seek consent as this is in itself a prohibited CEM as it seeks to establish a business relationship.
- Pre-ticked boxes and instances where the recipient does not have a choice or cannot give active consent, are not acceptable ways to obtain consent.
- Keeping a record of the consent is essential.
- ACMA recommends implementing**double opt-in**, i.e. where the subscriber confirms a subscription request by reply email or SMS before they are subscribed.

SPAM: SENDER IDENTIY

- CEMs must contain **accurate sender information**, including the individual or organisation who authorised the sending of the CEM and details of how the recipient can contact the sender.

SPAM: UNSUBSCRIBING

- CEMs must contain a **functional unsubscribe facility** where:
  - it must remain functional for at least 30 days after the original message was sent;
  - it must allow the unsubscribe message to be sent to whoever authorised the sending of the message, not necessarily any third party that sent it on their behalf;
  - unsubscribe instructions must be presented in a clear and conspicuous way;
  - a request to unsubscribe must be honoured within five working days; and
  - unsubscribing must be at low cost, or no cost, to the user.

SPAM: EXEMPTIONS

- Obligations to incorporate a consent and an unsubscribe function (but not the identity requirement) does not apply to Designated Commercial Electronic Messages (DCEM).

- A DCEM consists of purely factual information i.e. the message contains only factual information, a directly related comment (of a non-commercial nature), or the following limited 'commercial' information:

  - name, logo and contact details of the person who authorised the sending of the message;
  - name and contact details of the author of the message; or
  - name, logo and contact details of the author's employer, organisation, partnership or sponsor.

- A DCEM includes messages by a government body, registered political party, religious organisation, a charity or an educational institution messaging former or present students.

Katherine Sainty

Director
02 9660 9630
katherine.sainty@saintylaw.com.au
www,saintylaw.com.au
@SaintyLaw

Katherine is a corporate lawyer who specialises in digital, technology and media law

Sainty Law

Progressive commercial lawyers with market-leading expertise in the digital economy.