Mandatory Data Breach Notification
A guide to compliance

Will data breach legislation come into place?

- The Federal Attorney General's Department is currently considering industry submissions on the need and impact of federal data breach notification (DBN). Attorney General Mark Dreyfus is broadly supportive of the legislation.

- Australia's Privacy office has released a revised guide to complying with possible DBN rules which urges organisations to prepare in advance.

- Privacy commissioners agree that DBN rules are necessary. Some have hinted that Australian states may introduce their own rules.

When is data breach legislation likely come into place?

- The DBN is likely to form part of a suite of privacy reforms that come into effect from March 2014, however, the Government has acknowledged DBN reforms will not be in force at that time as "the industry will require sufficient time to adapt their systems".

- Proposed DBN laws in the European Union have allocated 18 months for affected organisations to comply from the date they would come into effect.

What will constitute a breach?

- The Federal Government is looking to overseas models to design its own DBN rules. Californian DBN law is considered the poster child of existing rules and is the most mature model.

- Californian DBN law defines a breach as a loss of a record that includes a customer's first name and surname along with a social security number; driver's license or identity card number, or bank account information including the necessary security or PIN codes to grant account access. It also includes loss of medical records and insurance information.

- The Federal Government will likely be initially conservative in setting what breaches need to be reported publicly.

What are the possible penalties?

- Reforms set to come into effect in March 2014 allow the privacy office to take small-scale offenders to court to face fines up to $22,000 for individuals and $110,000 for organisations. Repeat and serious offenders would face financial penalties of up to $220,000 for individuals or $1.1 million for organisations.

- Federal Privacy Commissioner Timothy Pilgrim said he could force organisations to patch identified flaws or adopt better security systems.

- Pilgrim says DBN laws should require organisations to report breaches to his office and in certain circumstances he wishes to retain the power to decide if affected individuals should be notified. He believes the privacy office should have the power to compel organisations to notify those affected.

How should organisations prepare and respond?

- The response to data breaches must be deliberate and systematic. Australian Information Commissioner John McMillan states that the "quality and effectiveness of the response can rank in importance alongside the gravity of the data breach". To this end, organisations should implement incident response mechanisms required to deal with data breaches, including a communications/PR policy that dictates how the organisation will deal with inquiries from the press and customers in the event of a breach. It must be tested and understood by all staff.

- SC Magazine recommends organisations begin by implementing the leading four recommendations of the DSD's Top 35 Mitigation Strategies.