Submission to the Serious Data Breach Notification Consultation

(Consultation closes 4 March 2016 — please send electronic submissions to privacy.consultation@ag.gov.au)

Your details

Name/organisation *(if you are providing a submission on behalf of an organisation, please provide the name of a contact person)*	Jo Stewart-Rattray Director International Board of Directors ISACA www.isaca.org
Contact details *(one or all of the following: postal address, email address or phone number)*	Australian Contact Details: [contact details redacted] ISACA Head Quarters: 3701 Algonquin Road Suite 1010 Rolling Meadows IL 60008-3105 United States

Publication of submissions

In meeting the Australian Government's commitment to enhancing the accessibility of published material, the Attorney-General's Department will only publish submissions to this website that have been submitted electronically.

Our preference is that submitters complete this template and send it to privacy.consultation@ag.gov.au.

However, if submitters choose to provide a separate document, the following formats are preferred:

- Microsoft Word
- Rich Text Format (RTF)
- txt format.

Please limit individual file size to less than 5MB. The department may create PDF documents from the above formats.

The department will still consider hardcopy submissions received by mail, but these submissions will not be published on the website.

Confidentiality

Submissions received may be made public on the Attorney-General's Department website unless otherwise specified. Submitters should indicate whether any part of the content should not be disclosed to the public. Where confidentiality is requested, submitters are encouraged to provide a public version that can be made available.

Would you prefer this submission to remain confidential? YES / (NO)

Your submission

On behalf of the more than 4,000 members of the Information Systems Audit and Control Association (ISACA) currently working in government, academia, and diverse industries throughout Australia, I would like to express our general support for the intent of the Privacy Amendment (Notification of Serious Data Breaches) Bill 2015. However, there are several topics that our community believes could be better addressed by the Bill.

In addition to my leadership roles within ISACA's international community, I have spent more than 25 years within the IT and Information Security fields in Australia. In my current role as Director of Information Security and IT Assurance with BRM Holdich, I have been fortunate to work across the breadth of Australia's private and public sectors, engaging in work with Australia's government, as well as our nation's utilities, banking and finance, higher education, retail and automotive manufacturing industries.

The great equalizer—for all of these diverse groups—is the security of their respective data, and the damage that data breaches can inflict. Consider the following: in 2013, a survey by the Australian Institute of Criminology found that 9.4% of persons surveyed had endured the loss or theft of personal information within the prior year; a survey last year by the Ponemon Institute found that, for Australia alone, business losses from data breaches had increased by nearly a third since 2010. In fact, it has been estimated that the annual economic impact of identity-based crimes in Australia exceeds $1.5 billion per year.

ISACA members throughout Australia, including myself, were pleased at the Australian government's proposed mandatory data breach notification legislation. The Bill, in its current form, is—in large part—a comprehensive measure that addresses the issue of data breach notification and is in keeping with legislative initiatives that have already been enacted, or are currently under consideration, in the United States, New Zealand, Canada, and the European Union.

However, one element is markedly absent from the provisions of the Bill. While the Bill calls for the required evaluation of a suspected data breach to occur, *it does not specify the qualities of the person or persons that should be evaluating that breach and reporting on it to the Commissioner.*

While the Bill is already strong, the inclusion of provisions that speak to the caliber of those evaluating these breaches is of extreme importance. When you are experiencing a sharp pain in your jaw, you do not consult a plumber; you turn to those best qualified and credentialed to assess the situation, and to advise you of the appropriate next steps. It is no different for data breaches. Those working in information security are uniquely qualified to evaluate the security 'health' of organizations, and to comprehensively and completely assess the extent and ramifications of data breaches. These information security professionals are also the best resources for determining what steps need to be taken to not only address a data breach, but to prevent similar breaches from occurring in the future.

One possibility for strengthening the Bill could be to insert provisions that provide guidelines that mirror, or at least approximate, the qualities and experiences deemed necessary by the Australian Signals Directorate's IRAP (Information Security Registered Assessors Program) when it verifies and endorses the qualifications of ICT professionals for work in government. Just to be able to be a member of IRAP requires five years' experience in ICT, with at least two years' experience in information security—in addition to professional certifications from a variety of internationally recognized and accredited organizations working in ICT and information security. This is a solid foundation in both ICT and information security, and it would align the provisions of the Bill with efforts already required by governmental programs such as IRAP.

Also, it should be noted that the most important step in conducting a risk assessment is establishing the context. The definition of 'serious harm' within the current version of the Bill is very high-level in nature, and more practical guidance could be given. This could take the form of something akin to the Commonwealth Government's Business Impact Levels. Additional guidance could also be provided in terms of what Australia considers as the rights to privacy a person currently enjoys. Providing practical guidance on this, within the legislation, would enable a more accurate appraisal of the harm of a related data breach.

Another element that remains unexplored in the Bill is the matter of ICT governance—a vital component for the effective coordination of ICT security risk management. Risk can be substantially reduced through effective ICT governance and management practices. This is, regrettably, an area which the Bill does not include, and we believe the Bill would be better for its inclusion.

The 'objective ordinary person test' outlined within the provisions of the Bill also gives cause for concern. The very nature of the Internet and rapidly advancing innovation in technology, particularly within the Internet of Things, is increasingly placing sophisticated services and tools at the disposal of the general public. While we understand the need for this legislation to anticipate the unknown, we feel that clearer guidance needs to be provided here, or we potentially set the stage for legal and other issues in this area in the future.

On behalf of ISACA's Australia member community, we wish to commend those whom have worked so diligently these past years to bring about Privacy Amendment (Notification of Serious Data

Breaches) Bill 2015. It is legislation that is vital and necessary, and greatly appreciated throughout the professional ICT and information security communities. We hope that you will consider the inclusion of the provisions and edits we have suggested, for it is our belief that it makes an already strong Bill even stronger, and ensures that the data of Australia's millions of people and businesses will receive the best stewardship and protection possible.