Privacy Case Study: Accident Compensation Corporation (ACC), New Zealand

Information Integrity Solutions P/L in conjunction with KPMG recently released an Independent Review of ACC's Privacy and Security of Information, which the ACC and the Office of the Privacy Commissioner, New Zealand commissioned.

The privacy incident that occurred created an enormous level of media interest and had serious implications for the ACC Board, its staff and senior political office holders. This report is ground breaking globally in the way in which it highlights that good privacy practice has to be tightly integrated into the operations of an organisation as a whole and is not simply something added on.

The data breach, which was the subject of the Independent Review occurred on 5 August 2011. It involved an email to a client with an attachment containing personal information on 6,748 of ACC's clients, including the details of the recipient of the email. The recipient only became aware of the attachment on 26 October 2011 and advised the ACC of the incident on 1 December 2011. Information Integrity Solutions and KPMG were engaged in March 2012 to conduct an Independent Review.

In the ACC's case, the Independent Review concluded that the breach that occurred was a genuine error, but that errors are able to happen because of systemic weaknesses within the organisation's culture, systems and processes. The subsequent "response process" could also have been better if appropriate policies, practices, escalation protocols and the "right culture" were in place to allow for transparency of breach handling at the appropriate levels, in an appropriate manner.

The lesson for all organisations, large and small; government or business is to be on their guard and manage a rapidly increasing risk, both to minimise the possibility of data breaches and have sound response strategies when they do occur.

Information is one of the most important assets in any organisation. Keeping information safe and unlocking its value while maintaining individual trust and confidence is one of the most difficult challenges facing organisations.

Where interaction with people and personal information is critical and central to an organisation's function, effective privacy management and a culture of respecting personal information must be a clear priority and given appropriate strategic importance.

An organisation's data needs to be protected by thorough and effective risk mitigation strategies to the same (or higher) levels as other vital assets. Without these strategies in place, the organisation is at risk of significant reputational damage.

While ACC defines privacy as everyone's responsibility, the design of systems and processes did not support a culture where the importance of personal information was valued and managed consistently and appropriately through the organisation.

Whilst there was a privacy officer supported by a small team, they dealt mainly with issues escalated from the branch network, rather than acting as a central coordination point for all privacy related matters across the ACC. There was no privacy program in place and accountability was not clear, including responsibility for escalating and resolving issues.

Systemic issues providing an environment for breach included:

- Dual monitor screens – working on more than one piece of work at the same time
- Extensive use of spreadsheets for management reporting
- Inconsistent organisational culture in regards to the importance of dealing carefully with personal information and a lack of clear accountability for addressing privacy issues.

Reducing privacy breaches begins with addressing all aspects of information handling. This includes processes for ensuring data quality and accuracy; access to data, reporting systems and through it all, an organisational culture that emphasises respect for individuals and the personal information that is collected, stored and used.

The importance of organisational culture was reinforced by external stakeholders where the overwhelming feedback was for client and client personal information to be treated with respect. What concerned them the most was the attitude of the organisation in dealing with personal information.

Risks associated with the collection and management of personal information were not a core part of ACC's risk management framework and historically privacy has not been a standing item on the agenda of the ACC Board and its sub-committees.

The Independent Review made a number of recommendations in relation to Board governance, leadership and privacy strategy, enhancing the privacy program, including treating security as a business issue, rather than an IT issue, with security owned by a member of senior management (outside of the IT function), organisational culture including having customer centric objectives, building privacy accountability and privacy by design or redesign into systems and processes.

In making its recommendations the Independent Reviewers emphasised the significance of a culture and environment where personal information is valued. This must be supported by an approach to compliance with the privacy principles that is embedded within governance, leadership and business processes and systems.

By Annelies Moens, CIPP/IT
Head of Sales and Operations, Information Integrity Solutions P/L and
President, iappANZ
annelies@iappanz.org