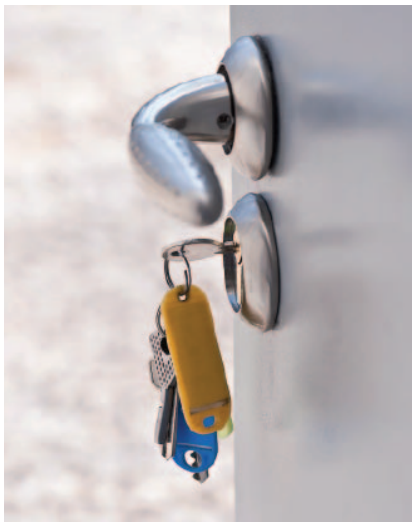
Corporate Lessons from Major NZ Data Breach



Some key lessons for organisations about corporate culture concerning privacy and security of information, have been provided by an Independent Review into a major data breach at New Zealand's Accident Compensation Corporation (ACC).

The data breach, the catalyst for the Independent Review, occurred in August 2011, after a manager inadvertently clicked and dragged an unrelated email so that it became an attachment to another message. The unrelated email included a spreadsheet containing "highly sensitive health information" about 6,748 ACC clients, including names, claim numbers plus conditions and details.

The ACC provides New Zealanders with personal accident insurance cover, dealing with a range of sometimes complex short and long term claims, requiring a substantial amount of health-related and personal information to be collected and assessed.

One ACC client involved, told the Independent Reviewers that there were 44 other alleged breaches, by the ACC, of legislation, guidelines or codes.

New Zealand's Office of the Privacy Commissioner (OPC), in conjunction with the ACC Board, requested the formal review, by KPMG Partner Souella Cumming and Malcolm Crompton, Managing Director of Information Integrity Solutions P/L (IIS) and former Australian Privacy Commissioner.

150 interviews

The Independent Review teams conducted more than 150 interviews with ACC staff and its full report published in August 2012 can be found at - http://www.iispartners.com/downloads/22-August-2012-ACC-Independent-Review-FINAL-REPORT.pdf. The significant data breach happened on 5 August 2011 but did not become public, through the news media, until March 2012.

The Independent Reviewers found that the breach was caused by "a genuine" human error, but "certain systemic issues as well as contributing factors led to the breach and, if not rectified, could lead to additional occurrences of significant privacy breaches".

The Report said these systemic issues included:

- Technology and business practice issues, including extensive use of spreadsheets for management monitoring and reporting purposes and desktop configuration that allows multiple monitors to be open at any one time.
- A culture where the importance of personal information and respecting individual's personal information is not consistent and is often de-emphasised over dealing with the management of the claim.
- Privacy management, including lack of clear accountability for addressing privacy issues when they are raised (including investigating and following up on issues) and for ensuring that client issues, including privacy matters, are dealt with in a holistic way.

Lack of clear accountability

The independent reviewers found that an "analysis of the events and steps taken by ACC highlighted systemic issues that increased the likelihood of the breach occurring, including the use of dual monitor screens, extensive use of spreadsheets for management reporting, a variable culture in regards to the importance of dealing carefully with personal information, and a lack of clear accountability for addressing privacy issues."

Other ACC vulnerabilities highlighted by the independent reviewers, were that current work practices and the wide range of policies and procedures, had led to an ad hoc approach to managing personal information.

Other vulnerabilities included:

- Some work practices (physical file copying and distributing physical files in response to access requests) and system design (such as open access to the majority of client data once staff have access to the claims management system) can result in inappropriate disclosure of personal information when not reinforced by a culture where the importance of personal information is understood, where all staff feel both supported in their work and also individually responsible, where staff are aware of the risks, and where sound management is appreciated and the consequences of not managing personal information appropriately are clearly defined.
- Business processes and systems would benefit from a comprehensive review to ensure privacy is built-in not built-on, and advances in technology (such as information portals) can be used to make personal information available to individuals while still ensuring high standards of access and protection on how the information is accessed and used.

The report stated that: "In agencies such as ACC, whose interaction with people and personal information is critical and central to their function, effective privacy management and a culture of respecting personal information must be a clear priority and given appropriate strategic importance".

"The impact of the information revolution on ACC means that the value of the personal data in its custody is increasing rapidly, with a commensurate impact on the risk exposure of ACC both in regards to data breach and the respectful management of personal data. Both point to the need for a renewed emphasis on governance of personal data including its risk management," the report said.

Clear message

In a clear message to all institutions, the Independent Reviewers said that: "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".

The nature of ACC's operations, the number of complex and long-term claims, combined with the manual nature of many of its processes and technology systems, has resulted in ACC having a history of privacy breaches and complaints," the Report said.

Information is increasingly the most important asset in an organisation, and, without proper management, is a rapidly escalating risk. The Report highlights that good privacy practice has to be tightly integrated into the operations of a corporation as a whole and not simply something added on.

In presenting the Report, IIS and KPMG 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, business processes and systems".

For more information please contact: Malcolm Crompton, Managing Director or Annelies Moens, Head of Sales and Operations, Information Integrity Solutions P/L on +61 2 8303 2438 or email amoens@iispartners.com

Download the Full Report:
http://www.iispartners.com/downloads/22-August-2012-ACC-Independent-Review-FINAL-REPORT.pdf.

Information Integrity Solutions P/L Top 5 lessons for private and public sector organisations:

— **Trust:** Engender trust with your citizens and customers by developing a culture, plus governance and leadership structures that support a privacy program to protect personal information. Individual trust in organisations is directly related to the level of control they have over their information, or the level at which the organisation has it 'under control'.

— **Culture:** Foster and develop an organisational culture that emphasises respect for individuals and the personal information that is collected, stored and used. Give this culture appropriate strategic importance and priority.

— **Leadership:** Appoint a member of the executive to be accountable and responsible for privacy. Implement mechanisms for ensuring that privacy best practice and compliance is built into all systems, products and services.

— **Privacy Program:** Build a privacy program to strengthen privacy management which minimises data breaches. Have sound response strategies when they do occur. Reducing privacy breaches begins with addressing all aspects of information handling.

— **Governance:** Include privacy vision and strategy as a board imperative. The data your organisation holds needs to be protected by thorough and effective risk management strategies to the same (or higher) levels as other vital assets. Without these strategies in place, your organisation is at risk of significant reputational damage.