Privacy risk management – what's it all about?

Privacy Commissioner John Edwards

iappANZ seminar

21 July 2015

KPMG Centre, Auckland

Privacy risk management - Growing global awareness

- International technology and market research company, Forresters, predicted 2015 as the year privacy and security became competitive differentiators.
- The law firm, Simpson and Grierson, recently advised its clients that while last year was all about health and safety, this year data protection and privacy should be on every boardroom agenda.
- Organisations worldwide are investing a great deal of resources in getting their personal information and data protection practices up-to-date and future-facing.
- iappANZ - commendable efforts to raise the profile of this topic.

International developments in privacy risk management

- Globally, we can see a number of initiatives and activity in privacy risk management. It is part of what appears to be a growing trend.
- One example of this, and it is a carefully and fully articulated model, has been developed by the Centre for Information Policy Leadership (www.informationpolicycentre.com).
- The Centre for Information Policy Leadership is a global think tank located in the law firm of Hunton & Williams LLP. Headquarters are in Washington, DC.
- The Centre's stated aim is to lead the way in initiatives to develop solutions to information policy issues that are practical, innovative and grounded in a deep understanding of technology and evolving business processes.
- The Centre has invested major resource in the privacy risk management area.

- Centre has launched a multi-year project on a risk-based approach to privacy: the Privacy Risk Framework Project. Key players – Bojana Bellamy and former UK Information Commissioner, Richard Thomas.
- Of course the context will not be a perfect fit for the New Zealand law and business environment. But I believe the underlying concerns will be familiar to you, and the proposed strategies may be of value. It may provide you with one or two useful tools to employ to good end within your organisations.
- "Risk management does not alter rights or obligations, nor does it take away organisational accountability. On the contrary, it has proven a valuable took for calibrating accountability, prioritising action, raising and informing awareness about risks, and identifying appropriate mitigation measures." (Paper 2: The role of Risk Management in Data Protection, p3).
- I have available the first of the Centre's papers on privacy risk management, in hardcopy, for those who are interested. It was produced in mid 2014. The second paper came out in November last year. All the papers are available on the Centre's website: https://www.informationpolicycentre.com/Privacy_Risk_Framework/

What does the Privacy Risk Framework involve?

- "The Privacy Risk Framework Project aims to bridge the gap between high-level privacy principles on the one hand, and compliance on the ground on the other, by developing a methodology for organisations to apply, calibrate and implement abstract privacy obligations based on the actual risks and benefits of the proposed data processing."
- Aim is to develop a *practical* framework to identify, prioritise and mitigate privacy risks effectively.
- Primary focus should be on *significant* privacy risks for individuals. "In other words, in a given situation, the question should be whether there is **a significant likelihood that an identified threat could lead to a recognised harm with a significant degree of seriousness**."
- A risk-based approach will usually take the organisation beyond legal compliance.

Privacy risk management - Key elements

What are the underlying key elements of privacy risk management?

- Perception (valid; reliable; comprehensive)
- Expectation management (say what you'll do and then do that)
- But – another key thing. All risk is not created equal. (Don't spend big $$$ to mitigate small fry risk.)

Privacy statements and Priv-o-matic

- How do you manage expectations in a practical way? Tell people what you are going to do with their information.
- In a marketplace where there is little difference in price for the good or service, a simple, clearly explained privacy statement will help to differentiate your business over another one.
- **New tool to help: Priv-o-matic – an automated privacy statement generator.** Estimated time to generate a privacy statement? 5 minutes. Aim is to make it easy for the smaller business owner to get online and get it sorted. Check it out. (www.privacy.org.nz)
- We see examples of this trend all around the world. Just look at Apple and Facebook. Although both have come under criticism at times for privacy issues, both now offer products and features directly responsive to marketplace calls for easily accessible privacy options and security, including encryption.

Grow a culture of awareness

- Effective privacy risk management will depend on having solid organisational support and structure.
- One of the foundational elements effective risk management is to have an organisational culture that has good levels of awareness. That awareness encompasses:
    - an understanding of the way your organisation uses personal information
    - an understanding of the 'information lifecycle'
    - an appreciation of typical areas of legal risk
    - a willingness to consider mitigating strategies and effective remedies when things go wrong.
- Awareness can be a tough thing to develop across a complex organisation.
- One of the key roles that my office plays is education. We have education for both organisations and consumers.

- **Online privacy training modules – Privacy 101; Health 101; Now: Approved Information Sharing Agreements. Next: Privacy Impact Assessment.** (Then: data breach notification; positive credit reporting; frontline staff)

Privacy Officers

- Privacy Officers are of course a vital component in any risk management strategy.
- Think about your privacy officer (maybe it is you?) how are they empowered in your organisation?
- How is privacy responsibility dispersed throughout your organisation? Think about your governance structures.
- Is there a better / more effective / way?

Privacy Impact Assessment

- To 'manage risk' – need first to have awareness of weak points and threats. How to develop that awareness?
- **Our new Privacy Impact Assessment handbook – now online**
- Doing something that changes your business processes?
- Introducing a new business practice?
- Using information in a new way?
- Developing a joint product with another agency? Sharing customer data?
- Think PIA – a tool to help you manage risk.
- The Handbook is divided into two parts. The first part helps you to decide if a Privacy Impact Assessment is even needed. The second part leads you through the steps involved in completing a PIA. There are templates at the relevant points that you can use as the basis for your own document.

Mandatory data breach notification

- When things go wrong you need a strategy.
- Safe to expect that your organisation will encounter data breaches.

- Mandatory breach notification – a recommendation made by the Law Commission and accepted by the New Zealand Government. (Similar legal requirements in other jurisdictions.)
- Already we are seeing voluntary data breach notification being adopted in NZ. (Examples: larger corporates; banks; government departments)
- Law change in this area would be a game changer. Why? It shifts business expectations; creates level playing field.

Conclusion

- **These are the sorts of things that I will be looking for in the event that things go wrong:**
    - Organisational culture and awareness
    - Trained staff
    - Sensible, clear policies and privacy statements
    - Use of privacy impact assessment
    - Engaged privacy officers
    - Awareness of data breach notification and mitigation
    - A risk management framework backed up by effective governance
- If we are investigating a complaint against your organisation, these elements will become relevant.

_____

Added impetus

Note two general but true statements.

One: Successful businesses have the trust and confidence of their customers.

Two: Having customers' personal information gives an organisation a competitive edge.

- Trust and confidence are foundations of a well functioning economy. Respect for customer data is essential for the maintaining trust and confidence in business. Our lives are becoming ever more enumerated and dissected.
- As you well know, the organisations that you represent have an obligation and a responsibility to manage and protect personal information. If people can't trust the

organisations they do business with to look after information that is about them, there can be no business.

A privacy manager at a major corporate told us that in her organisation's experience, nine out of ten data breaches are caused by human error - because of insufficiently trained staff or flawed processes.

That can be very damaging to a business in an age where consumers can switch service providers with a few mouse clicks or a telephone call. Being careless or complacent with personal data has financial, economic and legal implications.

Evidence? The cost of getting privacy wrong has become more expensive – not solely reputational.

Recent Human Rights Review Tribunal Privacy Act decisions:

- Hammond vs NZCU Baywide - $168,000 damages
- Taylor vs Orcon - $25,000
- Watson vs CCDHB - $15,000