Privacy and data breaches – how information governance minimises the risk

Preventing data privacy breaches is becoming increasingly important, with the increasing costs of dealing with cyber attacks, IT security breaches, and the subsequent legal actions and regulatory investigations. Strong IG, including privacy governance, is the most effective way to put in place robust systems to prevent and minimise privacy breaches, as well as respond to any privacy breaches that may occur.

Cyber attacks and privacy breaches

There is general awareness of the increase in cyber security attacks on organisations, and the significant risks that this poses to enterprise information security, legal and regulatory obligations, as well as the significant costs and reputational issues that result.

It is regularly reported that cyber attacks and data breaches are on the rise. The Identify Theft Resource Center Breach reported that US data breaches hit a record high of 783 in 2014, which was a 27.5% increase over the previous year, with over 85 million records exposed.[1]

Telstra's Cyber Security Report[2] states 'nearly a quarter of all the organisations we surveyed had suffered some kind of business interruption due to an IT security breach during the last 12 months. When that time frame was stretched to five years the figure climbed to nearly 60%. … The majority of Australian organisations we surveyed reported that they detected some sort of attempt to breach their IT security on a weekly or monthly basis.'

High-profile cyber security attack incidents include:

- Anthem – in February 2015 the second-largest health insurer in the US reported that stolen data included names, addresses, dates of birth, social security numbers and employment and histories of 80 million current and former customers;
- Sony Pictures cyber attack in late 2014, in which vast amounts of data was stolen, including personal information of employees, such as salaries, social security numbers, birth dates, medical records; emails; contracts; copies of unreleased films; and reports that hard drives were wiped leading to the shut down of Sony's computer systems for more than a week[3]. The attack was condemned by the US, Australian and other governments;
- JP Morgan Chase – in late 2014 the names, addresses, phone numbers and email addresses of 83 million households and small business accounts were stolen;
- Home Depot – in 2014 the theft of 56 million customer email addresses and payment card details;

[1] Data Breach Reports, Identify Theft Resource Center, 31 December 2014.
[2] Telstra's Cyber Security Report, December 2014, p30.
[3] 'US investigators suspect North Korea hired hackers for Sony hack', *The Age*, 31 December 2014.

- Adobe – in late 2013 the theft of 153 million customer records; and
- Target – in late 2013 the malware attack that compromised 70 million Target customer accounts and 40 million credit cards at its point of sale systems.

Costs of privacy breaches

The costs of a data breach will depend upon on its type and scale. However, for some large-scale breaches, the costs may run into hundreds of millions of dollars.

The direct costs of data breaches include the following:

- cost of investigating the breach;
- cost of wages through overtime and/or increased number of staff to deal with IT issues around security breach identification and remediation;
- costs of external advisors, such as IT security experts and lawyers;
- business interruption costs, particularly where access to computer systems is limited, either because of damage to systems or systems being shut down for remediation;
- costs of dealing with breaches – e.g., new replacements credit cards being issued where customer details of credit cards are stolen, and legal claims and pay-outs for data breaches; and
- costs of new IT and new processes and systems to prevent future privacy and data breaches.

There are also the indirect costs arising from data breaches, such as loss of reputation and potential loss of future customers, due to a lack of trust that customers' personal information will be kept safe.

Direct cost – case examples

In the US, Target reported in late 2014 that it had incurred $248 million in data-breach-related expenses and would receive $90 million from insurance policies.[4] This included costs for defending or settling more than 100 legal actions against it. Independent sources estimated that fraudulent charges ranged from $240 million to $2.2 billion.[5] In March 2015 a US court gave preliminary approval to a $10 million settlement of a class action to enable customers affected by the breach to be awarded up to $10,000 each in damages.[6] In April 2015, Target announced it had reached agreement with Mastercard to fund up to $19 million in payments to Mastercard issuers affected by the data breach, conditional on at least 90% of card issuers accepting the offer.[7]

[4] Weiss, Miller, 'The Target and Other Financial Data Breaches: Frequently Asked Questions', *Congressional Research Service Report,* 4 February 2015, p6.
[5] Weiss, Miller, 'The Target and Other Financial Data Breaches: Frequently Asked Questions', Congressional Research Service Report, 4 February 2015, p6
[6] Tabuchi, '$10 million Settlement in Target Data Breach Gets Preliminary Approval', The New York Times, 19 March 2015.
[7] 'Target Announces Settlement Agreement with MasterCard; Estimated Costs Already Reflected in Previously Reported Results', media release, 15 April 2015.

Home Depot reported it had paid $43 million in data-breach-related expenses and anticipated $15 million in insurance payments, and that at least 44 legal actions had been filed in the US and Canada.[8]

Regulatory sanctions

Globally regulators are imposing stiff sanctions and fines for data and privacy breaches. In addition to fines, regulators often impose requirements for organisations to conduct reviews, audits and provide ongoing compliance reports to the regulator. This can be a substantial ongoing cost, particularly where it may involve the unbudgeted expense of new or improved IT, increased cost of appropriately qualified personnel, particularly privacy experts and/or independent third-party audits, and ongoing compliance reporting.

United States

In the US, in April 2015, AT&T was fined $25 million for a data breach by the Federal Communication's Commission in its 'largest privacy and data security enforcement action to date'.[9] The data breaches involved the unauthorised disclosure of almost 280,000 of customer names, full or partial security numbers, due to employees accessing without authorisation customer records at AT&T call centres in Mexico, Colombia and the Philippines. Under the terms of settlement, AT&T is required to appoint a senior compliance manager, who is a certified privacy professional, to conduct a privacy risk assessment, implement an information security program and provide regular training to employee's on AT&T's privacy policies. AT&T is required to file regular compliance reports with the FCC.

United Kingdom

In the UK in 2012, the Brighton and Sussex University Hospitals NHS Trust received the largest-ever fine imposed by the Information Commissioner's Office (ICO), of £325,000. A contractor had been retained to destroy data on around 1000 computer hard drives containing confidential patient information. An individual sub-contractor removed some of the hard drives and without wiping the drives sold them on eBay.

In 2013, the ICO imposed a fine of £250,000 on Sony Computer Entertainment Europe, following a cyber attack on the Sony PlayStation Network Platform in April 2011 that compromised the personal information of millions of customers.

In 2013/2014 the ICO issued £1.97 million civil monetary fines.[10] The fines levied in the UK are set to increase once the new EU General Data Protection Regulations are enacted.

European Union

The draft Data Protection Regulation was issued in 2012, and the EU's European Council is aiming for its adoption in late 2015 or early 2016. After a transition period of two years, it will have immediate effect on all EU member states.

---

[8] Weiss, Miller, 'The Target and Other Financial Data Breaches: Frequently Asked Questions', Congressional Research Service Report, 4 February 2015, p7.
[9] 'AT&T to Pay $25 Million to Settle Consumer Privacy Investigation', Federal Communications Commission media release, 8 April 2015.
[10] Information Commissioner's Officer Annual Report and Financial Statements 2014/14, p24.

The draft EU Data Protection Regulation provides for sanctions and fines as follows:

- a written warning of cases of first and non-intentional non-compliance;
- regular periodic data protection audits; and
- fines of up to 5% of annual global revenue or €100 million, whichever is greater.[11]

Australia

The powers of the Office of the Australian Information Commissioner (OAIC) include:

- conducting assessments of privacy compliance;
- accepting enforceable undertakings; and
- seeking civil penalties, in the case of serious or repeated breaches of privacy, of up to $340,000 for individuals and $1.7 million for organisations.

The first enforceable undertaking under the new privacy laws that came into effect in Australia in March 2014 was entered into by Optus in March 2015, following a lengthy investigation by the OAIC. It was concerned that Optus did not have reasonable steps in place to safeguard the personal information held in its systems at the time the three significant incidents occurred, and as required by Australian Privacy Principle (APP) 11. The three incidents were:

- a change made to Optus's website, resulting in the names, addresses and mobile numbers of 122,000 of its customers who had elected not to have their details listed in a telephone directory being published in the White Pages;
- Optus made a change to its network that meant customers using the relevant modems it had provided who did not change the default user name and password were vulnerable, potentially allowing a person to make and charge calls as though they were the Optus customer; and
- a flaw in Optus's security processes led to certain customers whose voicemail was not password protected being vulnerable to 'spoofing' attacks, including accessing and using customer voicemail account messages, and preferences and settings being changed.

The Privacy Commissioner referred to the positive way in which Optus worked with the OAIC to address the incidents, and considered 'the enforceable undertaking was an appropriate outcome that will ensure Optus takes steps to strengthen its privacy controls and meet its security obligations under the Privacy Act'.[12] The enforceable undertaking required Optus to:[13]

- Engage a qualified independent third party to complete specified reviews and certifications. This included, for example,

[11] Article 79 of *Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data* (General Data Protection Regulation), Inofficial consolidated version GDPR, Rapporteur Jan Albrecht, October 2013.
[12] Office of the Australian Information Privacy Commission media release, 27 March 2015.
[13] Singtel Optus: enforceable undertaking, Office of the Australian Information Privacy Commission, Enforceable Undertakings www.oaic.gov.au

'a. review of the additional security measures Optus adopted in response to the Privacy Incidents ('Review A'). These additional security measures include:

i. Enhancing Optus's monitoring program of change management that has the potential to affect the security of its customers' personal and sensitive information;

ii. Enhancing Optus's penetration testing: for fixed and mobile services; on all major IT projects as part of Optus's Security Risk Assessment process; and as part of its annual monitoring program.

b. a review of Optus's vulnerability detection processes across the organisation concerning the security of personal information;'

- provide copies of those reviews and certifications to the OAIC;
- implement any recommendations and rectify deficiencies identified in those reviews and certifications; and
- provide a report by an independent third party to the OAIC certifying that the specified actions had been completed.

Privacy governance framework

In light of the costs and time involved in responding to data breaches and the subsequent ongoing consequences and expense, there is a strong incentive for organisations to ensure they have an appropriate privacy framework in place, both to prevent privacy breaches and to respond to any data and privacy breaches that may occur. As part of good corporate governance to manage risk, the privacy framework should be part of a robust overall information governance framework to manage all information and data throughout an organisation.

The New South Wales Information and Privacy Commission, which covers state public sector agencies, has published a *Privacy Governance Framework*.[14] The framework enables a holistic organisational approach to the management of personal information, draws upon the 'privacy by design' principles, and consists of five elements (as shown in the diagram below): setting leadership and governance; planning and strategy; program and service delivery; complaint incident management; and evaluation and reporting.

[14] Privacy Governance Framework Resources, www.ipc.nsw.gov.au

Privacy by design – the seven principles

The objectives of 'privacy by design', developed by Dr Ann Cavoukian, former Information and Privacy Commissioner in Ontario, are aimed at ensuring privacy and gaining personal control over one's information, and, for organisations, gaining a sustainable competitive advantage. The benefits of the 'privacy by design' approach has been recognised by information and privacy regulators, including in the United Kingdom and Australia. The seven foundation principles are:[15]

Proactive, not reactive

The privacy by design approach is about proactive, rather than reactive, measures. It anticipates and prevents privacy-invasive events.

Privacy as the default setting

It seeks to deliver maximum privacy, by ensuring that personal data is automatically protected in any IT system or business practice. No action is required by an individual to protect their privacy – it is built into the system, by default.

Privacy embedded in design

Privacy is embedded in the design and architecture of IT systems and business practices, rather than being an add-on. Therefore, it is an essential component of the functionality.

Full functionality – positive-sum, not zero-sum

Privacy by design seeks to accommodate all legitimate interests and objectives in a positive-sum 'win-win' manner, not through a zero-sum approach, with unnecessary trade-offs. *It demonstrates it's possible to have both* privacy and security.

End-to-end security

Having been embedded in the system before the first element of information being collected, privacy by design extends throughout the entire lifecycle of the relevant data. This ensures that at the end of the process, all data is securely and quickly destroyed.

Visibility

Privacy by design means that, whatever business practice or technology is involved, it is operating according to the stated promises and objectives, subject to independent verification. Its components and operations remain visible to users and providers alike.

Keeping user privacy user-centric

Architects and operators are required to keep individuals' interests uppermost, by offering, e.g., strong privacy defaults, appropriate notice, and user-friendly options.

[15] Dr Ann Cavoukaian, 'Privacy by Design, The 7 Foundational Principles', revised January 2011 www.privacybydesign.ca

Benefits of 'privacy by design'

The ICO has set out the benefits of designing projects, processes, products or systems with privacy as a consideration at the outset:[16]

- Potential problems are identified at an early stage, when addressing them will often be simpler and less costly.
- There is increased awareness of privacy and data protection across organisations.
- Organisations are more likely to meet their legal obligations, being less likely to breach relevant legislation or regulations, such as the Data Protection Act 1988 (UK), the Privacy Amendment Act 2012 (Aus)(C'th) or the EU's Data Protection Directive.
- Actions are less likely to be privacy intrusive and have a negative impact on individuals.

Privacy at the outset

It is clear that the most efficient way to ensure privacy protection is for it to be included and embedded in the early stages of any project or new product or service, and for this to continue throughout its lifecycle. The ICO recommends that privacy and data protection be considered when: [17]

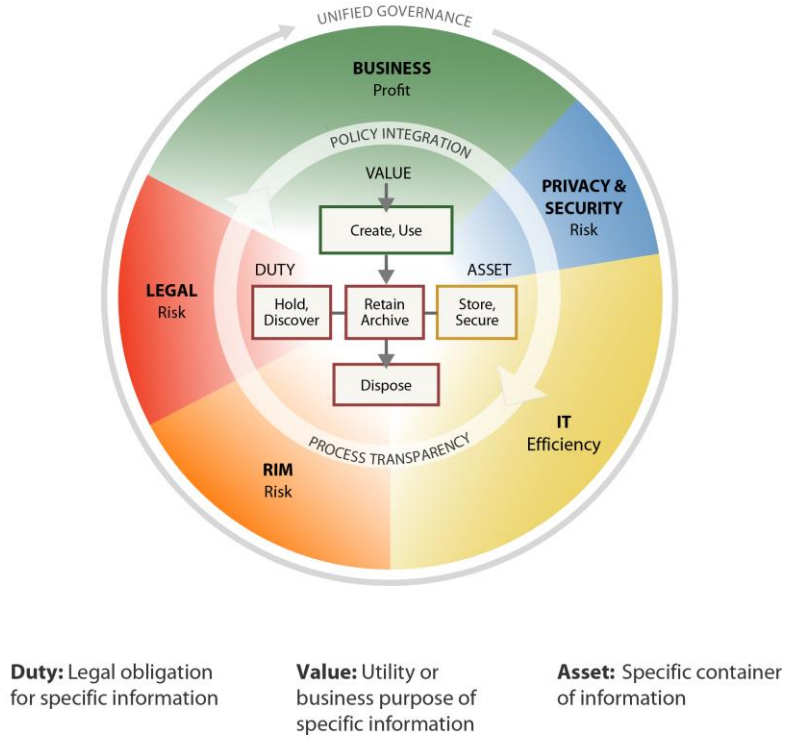
- building new IT systems for storing or accessing personal data;
- developing legislation, policy or strategies that have privacy implications;
- embarking on a data sharing initiative; or
- using data for new purposes.

Privacy as part of IG

While it is important to have a strong privacy framework, it needs to be supported by robust information management and governance throughout the organisation. The NSW Privacy Commissioner states, '[p]rivacy is easiest when it is the organisation's standard mode of operation and monitoring is mainstreamed through existing governance mechanisms such as the Board, Executive of Senior Management meetings. Monitoring and review can be achieved through existing mechanisms such as the Audit and Risk Committee or Customer or other Advisory Committees.'[18]

The Information Governance Initiative describes IG as a co-ordinating list of information activities, including information security, compliance, data governance, risk management and privacy.[19] IG is defined as: 'the activities and technologies that organisations employ to maximise the value of their information while minimising associated risks and costs'.[20]

[16] Information Commissioner's Office, Guide to Data Protection, www.ico.org.uk
[17] Information Commissioner's Office, Guide to Data Protection, www.ico.org.uk
[18] Dr Elizabeth Coombs, NSW Privacy Commissioner, 'Why Privacy Governance?', Privacy Governance Framework Resources, www.ipc.nsw.gov.au
[19] Information Governance Initiative Annual Report 2014, p13.
[20] Information Governance Initiative Annual Report 2014.



The Information Governance Reference Model (IGRM) provides a framework for defining a unified governance approach to information, including privacy[21]. It shows information is a cross functional challenge, requiring collaboration between the various stakeholders within an organisation (i.e., privacy, information technology, legal, records management and business units), and highlights the intersection and dependence across these stakeholders.

Benefits of IG

The benefits of a holistic approach to IG, including privacy governance, are:

- senior-executive-level engagement and decision-making on important strategic opportunities and risk mitigation issues concerning organisational information, including privacy considerations;
- improved management of data, with more efficient retrievability of data retained;

[21] Information Governance Reference Model (IGRM) Guide, E.D.R.M, www.edrm.net

- defensible destruction of redundant, outdated and trivial data/information, with an audit trail that can be relied upon in litigation**.** In the privacy context, it means old or outdated customer records are disposed of and are no longer held by an organisation;
- improved selection and return on investment on new technology, appropriate to the organisation's legal, compliance and business needs. This means technology investment is a strategic priority, with appropriate budgets and investment plans leading to long-term cost efficiencies. This is in contrast to a reactive unplanned expensive plug to a data and privacy breach crisis, with the consequent legal and IT costs of responding to a data breach, as well as increased costs of ongoing compliance that may be imposed by a regulator;
- comprehensive and aligned policies, processes, people and response plans. This includes comprehensive ICT security and privacy breach response plans, as well as awareness training of policies and processes, and training to deal with a cyber attack and privacy and data breaches; and
- reduced costs and increased efficiencies arising from the implementation of an aligned strategy and policies, in contrast to the inefficiencies of the traditional fragmented siloed approach. A good example in the privacy context is including 'privacy by design' principles at the outset of projects, new processes, new products or services, or when using data for new purposes.

Conclusion

Having a strong privacy and information governance framework properly embedded in an organisation should prevent and minimise privacy and data breaches. To have robust governance, consider:

- reviewing current privacy and information governance frameworks and assessing whether they are aligned to achieving organisational objectives and meeting best practice standards in information management, including data and privacy protection;
- reviewing and updating privacy policies and processes;
- embedding 'privacy by design' for projects, processes, new products and services;
- embedding privacy and data protection when developing new IT systems for storing or accessing personal information;
- developing or reviewing privacy and data breach incident response plans to ensure they are current, including notification processes to regulators – such as, the OAIC Data Breach Notification Guide; and
- training of relevant personnel to enable the organisation to respond adequately in the event of privacy and data breach – this will include IT, communications, privacy and legal personnel.

If you would like assistance reviewing your current privacy and information governance ecosystem, please contact Susan Bennett, Principal, on +61 2 8226 8682 or email susan.bennett@sibenco.com.

This article is for reference purposes only and does not constitute legal advice.