Why information governance needs top-down leadership

By Susan Bennett, Principal, Sibenco Legal & Advisory

- The exponential growth in data and digital disruption is a key driver for strong information governance.
- Information governance is about delivering value to the business's bottom line, as well as minimising risk and costs.
- Information governance systems and processes need to align with the organisation's overall strategic business objectives.

Effective leadership of information governance (IG) is key to ensuring that appropriate strategies, priorities, policies and processes are successfully embedded in an organisation, both to maximise the opportunities and minimise the risks arising from the information it holds.

A robust IG framework enables organisations to manage proactively the exponentially growing data and information they have. The main drivers of IG are:

- the value to the organisation derived from the data held within the organisation, which leads to improved performance and profitability — for example, using data analytics to mine 'big data', to create new or improved products or services
- minimising potential risks, which may otherwise lead to significant legal issues, business interruption, loss of productivity, costs and reputational damage — for example, cyber security attacks and privacy breaches.

What is IG?

The definition of IG is:

> The activities and technologies that organisations employ to maximise the value of their information while minimising associated risks and costs.[1]

This definition recognises that IG is about delivering value to the business's bottom line, as well as minimising risk and costs. Organisations are now continually facing both threats and opportunities from the ever-increasing growth of digital data (big data) and digital disruption (for example, online shopping, online education). This is causing organisations to find new ways to compete in the marketplace and to develop new business opportunities to drive profits; conversely, the exponential growth in data being held poses increased risks and costs to organisations.

The challenge is how to implement an effective IG framework, which will deliver both value and minimise risk, when information management activities are carried out by different business areas within an organisation and with different 'owners' within each of those areas.

Who is responsible?

Typically, an organisation's data and information is managed by various 'owners' — for example:

- compliance — risk and compliance director or chief risk officer
- eDiscovery/document production — eDiscovery counsel or general counsel
- information communication and technology security — chief security information officer, chief technology officer or chief information officer
- legal — general counsel
- privacy — chief privacy officer or general counsel

- records and information management — records and information manager.

Table 1 illustrates the broad range of different types of technologies used in information management activities, and highlights the different areas and senior managers typically responsible for information management across an organisation.

Where do the risks and costs arise?

The vast amounts of data held pose increased risks and costs to organisations, arising from:

- legal and compliance, particularly in relation to privacy obligations, with the growing focus on privacy arising from high-profile cyber security attacks and thefts of customer records
- information communication and technology (ICT) systems that prevent privacy and ICT security breaches
- the cost of production of documents in litigation and regulatory investigations
- record and information management (RIM) complying with legal and business requirements, where data is increasing exponentially, and retention policies may not be keeping pace with business operations and legal requirements.

Governance for information complexity

Boards and senior management are responsible for ensuring that appropriate governance frameworks, policies and processes for information management activities are in place and being adhered to, in order to manage risk appropriately. However, with the exponential growth of data, and changes to the way businesses operate caused by digital disruption, not only is it a challenge for governance to keep pace with new developments, it can be a challenge for boards and senior management to fully understand the opportunities and risks arising from all the information management activities throughout an organisation.

Organisations are increasingly concerned with preventing security breaches of enterprise systems, and are aware of the penalties for failing to comply with regulatory requirements such as customer privacy, as well as the potential for significant reputational damage to their brand.

Cyber breaches

There is general awareness of the increase in cyber security attacks on organisations and the significant risks that this poses for them. It is regularly reported that cyber attacks and theft of data are increasing. 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 per cent. Furthermore, 41 per cent of organisations reported that they had detected a major security breach in the last three years. ... 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. .... 38 per cent of organisations reported that their most recent attack was due to cyber-crime, with viruses accounting for 31 per cent, suggesting malicious hackers are becoming more active.'

High-profile cyber security attack incidents include:

- 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

Table 1: Technologies used in information management activities

Technologies	Area(s) responsible	Position(s) responsible
Data storage and archiving	Information technology	Chief technology officer (CTO) or information technology leader
Data mining (for marketing — eg improved customer service, development of new products)	• Marketing and/or • Business units and/or • Privacy – privacy or legal	• Chief marketing officer or chief digital officer (CMO, CDO) • Senior managers • Chief privacy officer or general counsel (CPO, GC)
Data mining (to improve business processes — eg reduce logistic costs)	Business units	Senior managers
eDiscovery	Legal	Discovery counsel/litigation counsel
Information, communications, technology security	Information technology	Chief information security officer (CISO), chief information officer (CIO) or chief technology officer (CTO)
Records and information management	Records	Records and information manager (RIM)
Risk and compliance	Risk and compliance or legal	Senior manager/GC

> The key to addressing and managing information/data throughout an organisation is to take a holistic approach driven from the board and the C-level down.

more than a week.[3] The attack was condemned by the US, Australian and other governments

- eBay — the theft of 145 million eBay user accounts
- Adobe — the theft of 153 million customer records from Adobe
- Target — the malware attack that compromised 70 million Target customer accounts and 40 million credit cards at its point of sale systems.

In light of the significant risks posed to organisations, it is essential that IG include the information technology architecture and system risks to ensure that:

- risks of breaches of organisations' information technology systems (that is, cyber security attacks) are minimised
- appropriate cyber incident and response plans are in place
- the relevant personnel are trained, and able, to respond adequately in the event of cyber breach — this will include IT, privacy and legal personnel.

Privacy breaches

Privacy breaches may occur as a result of a cyber attack where personal information is stolen, as in the above examples, or by the breaches within an organisation exposing it to regulatory and legal issues and costs. Organisations need to have in place effective policies and processes for the management of data breaches, including making notifications where required by regulatory bodies such as the Office of the Australian Information Commission (OAIC).

The Australian Privacy Principles (APP) regulate the handling of personal information for government agencies, and businesses with a turnover of more than $3 million (as well as some smaller businesses, such as health care providers). The APPs cover the collection, use, disclosure and storage of personal information.[4] The powers of the 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 $1.7 million.

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 APP 11. One of the incidents arose from a change made to Optus's website, resulting in the names, addresses and mobile numbers of about 122,000 Optus customers who had elected not to have their details listed in a telephone directory being published in the White Pages. 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'.[5]

Data analytics for marketing and product development

Another way in which organisations need to be mindful of and embed privacy is through the growing use of data analytics for mining of 'big data'.

Organisations now have a strategic focus on the use of digital technology as a tool to better service customers to meet market competition and improve profitability. They may use data analytics to improve business performance: for example, analysing data to improve logistics, or to improve or create new products or services. The importance of this focus is reflected in new roles such as chief data officer, chief digital officer and digital marketing manager.

However, if data analytics are carried out without regard to the privacy obligations of the information the organisation holds (in relation to its customers, students, patients, etc), there is a serious risk of privacy breaches and, potentially, reputational issues for the organisation. An effective IG framework will enable and embed effective cross-function information management processes and people, to ensure that value can be maximised while risks are minimised — for example, by ensuring that a new product team includes a privacy expert at a very early stage of a new product development, to make sure that privacy obligations are factored in and future privacy breaches minimised.

This is in contrast to a situation where products are developed without privacy considerations being taken into account (either partially or fully at the time of development), so that the privacy compliance and risks are managed through retrospective fixes at significantly increased costs.

The benefits of an IG framework

A sound IG framework is the critical foundation that enables organisations to govern and manage properly the information they hold. The benefits of a holistic approach to IG are:

- senior-executive-level engagement and decision making on important strategic opportunities and risk mitigation issues concerning organisational information
- increasing revenue and profits through the use of data analytics to develop or improve products or services, or through developing strategies to improve efficiencies and reduce costs
- improved management of data, with more efficient retrieval of retained data
- defensible destruction of redundant, outdated and trivial data/information, with an audit trail that can be relied upon in litigation
- improved selection and return on investment (ROI) on new technology, appropriate to the organisation's legal, compliance and business needs
- comprehensive and aligned policies, processes and response plans — including comprehensive ICT security and privacy frameworks and breach response plans
- 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.

IG framework and leadership

The key to addressing and managing information/data throughout an organisation is to take a holistic approach driven from the board and the C-level down.

Figure 1: Information Governance Reference Model (IGRM)

Linking duty + value to information asset = efficient, effective management

Duty: Legal obligation for specific information

Value: Utility or business purpose of specific information

Asset: Specific container of information

Information Governance Reference Model / © 2012 / v3.0 / edrm.net

In order for an IG framework to be successfully implemented and embedded in an organisation, there needs to be strong leadership and championing of IG from those in the key areas currently responsible for information activities.

In developing or reviewing a current IG framework, careful consideration needs to be given to the organisation's strategy and current situation, balanced against technology security priorities and legal and compliance obligations.

Board

To optimise the board's performance, it is essential that directors have a mix of skills and expertise. This includes one or more directors with skills in the following areas: cyber security architecture and systems; the relevant skills to contribute to the organisation's current and future strategy regarding digital disruption threats and opportunities; and legal and compliance expertise regarding information activities throughout the organisation, including privacy and record and information management.

Executive leadership

While it is important that boards and senior executives have a broad understanding, and be champions, of a robust IG framework, equally important is who will be responsible day to day for driving and implementing IG. This will vary between organisations, and is likely to depend on its strategic priorities, size, resources, and the current position of information management within it.

Examples of IG leadership are:

- **Steering committee** — a committee made up of the relevant C-level executives responsible for different areas of information management — for example, chief operating officer (COO), GC, CIO/CISO/CTO, CDO/CMO, CPO, RIM. A chair would be appointed to lead monthly meetings, and the committee would be responsible for setting overall strategic priorities, deciding on pilot projects, reviews of implementation, etc.
- **Current C-level executive** — an IG leader who is a current C-level executive, such as a CIO or GC

with the appropriate leadership skills, and some cross-functional expertise, to enable them to effectively lead IG — for example, a CIO with significant experience preventing and responding to cyber attacks and cyber security breaches, responding to regulatory and litigation production of electronic documents and data; as well as data analytic technologies for areas such as marketing, or a GC who has extensive experience in strategy and implementation of new technology systems and responses to major crisis or incidents such as cyber attacks and cyber security breaches. Whether an existing C-level executive is able to adequately lead IG will depend upon how their other responsibilities are managed (for example, by delegating more) and the organisation's strategic priorities, size, structure and resources.

- **Designated new C-level position** — a new C-level role as the chief information governance officer, as proposed by the Information Governance Initiative (IGI), a US IG think-tank. The IGI describes the CIGO's role as, 'to balance the stakeholder interests from each facet of IG and develop the right operational model for the organization.'[6] In building the case for a CIGO, the report explains that 'Chief Information Officers at most organizations are in fact only responsible for technology infrastructure, and not the information itself. Responsibility for the information is the raison d'être of the CIGO.'[7]

Leadership skills for effective IG governance

Whether the leader is an IG steering committee, a designated C-level executive within their current existing role or a CIGO, the task is to successfully align IG systems, processes and people to meet the organisation's overall strategic business objectives. For a robust and effective IG regime, the following is required.

Information governance checklist

- Are your leaders embedding IG as a foundation of good corporate governance?
- Do you have IG champions at board level?
- Do you know the IT and cyber risks for your organisation?
- Is the data held within your organisation being used effectively for multiple business value-creating purposes?
- Have you clearly articulated the purpose of a robust IG framework in your business?
- What is your organisation measuring — eg:
  - number of attempted cyber attacks; number of breaches of IT systems per quarter and per annum and cost of responding to breaches, business interruption, etc?
  - number of privacy breaches per annum and cost of responding to breaches, business interruption, etc?
  - revenue, cost, profit of new/improved products developed from information derived from analytics?
  - cost of implementation of new IT systems and software?
  - percentage of increase in data and percentage of data deleted per annum?
  - cost of production per page of reviewed documents for litigation and regulatory inquiries?
- Who is the day-to-day leader of IG? Is there a person clearly responsible or an IG steering committee?
- Where there is an existing or contemplated IG steering committee:
  - are all the relevant senior stakeholders on the committee?
  - are those committee members able to embed appropriate IG processes throughout the organisation to achieve strategic organisational objectives?
- Are those responsible for information management on a day-to-day basis able to work collaboratively across functions to ensure that IG strategic objectives are met and achieve best practice, with the resulting efficiencies?
- Do you have a clear and comprehensive IG framework that includes:
  - current policies and processes embedded within the organisation — in particular, is privacy embedded within your organisation?
  - IT policies and plans for disaster recovery and business continuity for cyber security incidents?
  - policies and processes that comply with current records retention legislation and regulatory requirements such as, OAIC Data Breach Notification Guide?
  - training of key personnel to implement policies and processes and execute cyber security plans?
  - regular reviews and audits of relevant cyber security, privacy, and records management policies and processes, etc?
- Can your IG framework and those responsible for IG adapt and respond promptly to changes in strategic organisational objectives — eg, to new business opportunities involving arising from opportunities through digital disruption or data analytics — or to regulatory change — eg, changes to privacy laws or records retention requirements?
- Do your policies and processes adequately cover:
  - employee cyber security education and awareness training?
  - social media use?
  - mobile device and BYOD use?
- Do you have external audits to ensure best practice standards in information management and adherence to policies and processes?

- **Strategic** — IG leaders need to be strategic thinkers, to implement an IG framework that will effectively respond to the increasing complexity of business and the interaction of technology and risk management. The chair of the committee or designated executive should be able to provide wise counsel (to a CEO or board committee or board) on business opportunities, information technology architecture and system risks, and the risks impacting activities within the organisation.
- **Alignment** — IG leaders need to align the IG framework to meet the organisation's strategic objectives. With rapid changes in technology requiring rapid changes to business processes in order to compete in the market, IG leaders will need to promptly review and adapt policies and processes, and ensure there is appropriate employee training and awareness, so that strategic business objectives are met and risks continue to be minimised.
- **Influence** — the steering committee or designated executive should be an effective influencer in all directions — up (for example, to CEO and board), across (to other C-level executives, for example, COO, CFO) and down the organisation (for example, to marketing, business units) — so that stakeholders understand the reason for decisions, and support and implement IG priorities, systems, policies and processes.
- **Innovation** — the steering committee or designated executive will need to recognise, assess, and support, where appropriate, innovative opportunities that create value for the organisation, as well as managing risk. This may include new models or policies for IG that better facilitate the achievement of business objectives while managing organisational risk. It is likely to include shifts from traditional structured policies and processes to better manage risk — for example, increased and different ways of engaging and training employees on appropriate use of social media, mobile devices (including BYOD), to reduce risk more effectively than outdated policies, draft policies or policies that are not yet universally agreed upon.
- **Collaboration** — the steering committee or designated executive is likely to embed a robust IG framework where people work collaboratively within teams and cross-functionally through the organisation on information management activities. This will happen where consensus is built, with the relevant stakeholders all working towards the same overall business objectives. Where rapid technological or business changes require a steering committee or designated C-level executive to get IG changes implemented quickly, it will require prompt buy-in and active support of the changes and the implementation actions required. This is more likely to be achieved and sustained in the long term when a culture of co-operation exists and there is an understanding of the need to align IG with business objectives to enable those objectives to be achieved.
- **Change management** — arguably, the most important skill a steering committee or designated executive will need for effective IG is effective change management. This is particularly the case where new business strategies are set that involve implementation of new technologies and/or new ways of doing business that impact information management activities and IG. For example, setting a digital strategy may involve a significant transformation in the way business is done — this is likely to require a number of leaders with strong change management skills to drive and implement the necessary changes.

Susan Bennett, can be contacted on (02) 8226 8682 or by email at susan.bennett@sibenco.com.

Notes

1 Information Governance Initiative *Annual Report* 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.

4 The 13 Principles are contained within Schedule 1 of the *Privacy Act 1988*.

5 Office of the Australian Information Privacy Commission media release, 27 March 2015.

6 Information Governance Initiative, *Annual Report* 2014, p28.

7 Information Governance Initiative, *Annual Report* 2014, p28.