THE GOVERNANCE OF THINGS –
Unpacking the Benefits of Information Governance

The Information Governance Imperative

Information Governance ANZ was launched to strong industry and media interest in August 2016 as information governance has become a key issue for organisations in today's security conscious world.

The imperative driving this surge in interest is twofold, but is essentially all about risk management:

1. The fast pace of the evolving digital world can disrupt existing businesses that don't have a proactive information governance program; and
2. Effective leadership of information governance is the key to ensuring appropriate strategies, priorities, policies and processes are successfully embedded in an organisation to maximise the opportunities and minimise the risks arising from the information it holds.

The value for organisations is to enable the delivery of better outcomes by minimising the risk and maximising the value of the information they hold.

The value to individual information governance professionals, is to keep them up to date with the latest developments and international global thinking and ensure the professional discipline of information governance is recognised as a key component to managing the exponential rise in data in the information age.

What is Information Governance?

While the concepts of information and governance are not new, the discussion around information governance has emerged as a necessary discipline to deal with the vast amounts of information being generated everyday by organisations. The challenge for organisations, whether in business, government or non-for-profit, is in developing a strategic, top-down approach to managing all aspects of information within the organisation.

This includes:

- What information is required to be held?
- What information the organisation can use to deliver benefits to the bottom line?
- Security of information – how it is and will be kept secure and how personally identifiable information is securely managed.

In short, Information Governance:

- Ensures that information is managed to achieve the strategic objectives of the organisation; and
- Provides the framework, systems and processes for ensuring the value of information is maximised and risks are minimised.

Cybersecurity and Information Governance

Relentless cyberattacks, the potential of data and privacy breaches and the ever increasing volume of information present enormous risk to organizations.

Significant cybersecurity investment, including the latest technology and best systems in place, is unlikely to prevent all breaches. And even if your cybersecurity technology and systems are first rate, there is always the issue of human failure – for example, employees leaving laptops or mobile phone in public places, or employees who download unauthorised software, or the problem of rogue employees and increases in information theft from within organisations.

In the event of a successful data breach the issues become - what information will be accessible to a cybercriminal, and what safeguards have you put in place in relation to sensitive data or data containing personal identifiable information?

A holistic and strategic approach to cybersecurity, privacy, records and information management is critical to ensure that data and privacy breaches are minimised.

Information as an Organisational Asset

Organisations need to consider information as an asset and measure both the value and costs of the data they hold. This means measuring the financial benefits derived from the value of data held as well the costs and subsequent savings from risk management investments.

ON THE VALUE SIDE

This includes investments in technology tools that can be used for competitive advantage and deliver benefits directly to the bottom line – such as:

- data analytics to improve or develop new services or products;
- data analytics to increase efficiencies in manufacturing processes;
- data analytics to improve delivery of services by government to citizens; or
- contract management technology to maximise financial returns of contracts;
- analytic tools for auditing to prevent or detect early fraudulent activity.

ON THE RISK SIDE

This includes strategic investments in technology and systems to minimise the risks and costs of data and privacy breaches arising from the exponential rise in the amount of data that is being held and stored by organisations, such as:

- systems and technology tools to reduce the amount of data being stored by organisations – that is, minimising the amount of redundant, outdated and trivial (ROT) data so there is less overall data;
- systems and technology to ensure that sensitive business data and information containing personally identifiable information has enhanced security and is more difficult to locate or access in the event of a successful cyberattack; and
- technology to search, identify, and review information in the discovery and production process in litigation and regulatory inquiries.

The Cost of Information

Is often only fully understood after the event, such as:

- Following a cyberattack and a data and/or privacy breach – with costs including business interruption costs, damage to reputation, potential regulatory investigation and litigation, including the costs of responding to regulatory investigations, potential sanctions and the cost of any litigation and subsequent pay-outs;
- Implementation of new technology system - with the additional costs incurred in dealing with excessive amounts of ROT, stored at additional cost. This is likely to delay implementation of a new system and impede management of information going forward unless addressed to accord with best practice information management;
- Litigation or regulatory investigations or commission of Inquiries - where the costs of document production are enormous due to the vast amount of data that needs to be searched, identified as relevant, reviewed and produced in accordance with legal requirements, or the potential sanctions and costs of not being to produce all documents that were required to be kept either in accordance with legal obligations or Legal Holds.

Join Information Governance ANZ

The emerging field of information governance requires the engagement of professionals from multiple disciplines, including cybersecurity, data analytics, data privacy, data governance, eDiscovery, information technology, information management, legal, privacy, records management, and risk and compliance.

We welcome all new Information Governance ANZ members, supporters and sponsors.

Join now at - www.infogovanz.com

THE BENEFITS of Information Governance

STRATEGIC SPEND OF TECHNOLOGY INVESTMENT

a strategic framework to ensure that technology investments are made in accordance with overall organisational strategic objectives and priorities

ASSUME CONTROL OVER THE DYSFUNCTION CREATED BY INFORMATION SILOS

a system which enables organisations to actively and firmly deal with the exponential amounts of data being created and efficient removal of ROT

IMPROVED ACCOUNTABILITY GIVES THE BOARD THE TRANSPARENCY NEEDED TO SIGNAL GREATER INVESTOR CONFIDENCE

a clear information strategy, enables the Board and C-Suite to have strategic oversight of the value of the organisation's information as well as the costs and risk management of information

EFFECTIVE MEASUREMENT OF BENEFITS FOR BUSINESS CASE JUSTIFICATION TO DRIVE FUTURE INNOVATION

measurement of benefits and costs to the bottom line derived from the information held, such as a new product developed through the use of data analytics, or the costs to the organisation from a data privacy breach.

MEET COMPLIANCE OBLIGATIONS SEAMLESSLY

systems and processes ensure that information is kept in accordance with record keeping obligations and essential documents needed for business purposes, but that ROT is actively managed and removed from the organisation