IRON MOUNTAIN®

LAW & CYBER

Whitepaper in partnership with Law & Cyber

Information transformation: Your best defence against a data breach.

September 2023

Contents

Introduction

Data is now regarded as the world's most valuable resource.

While many have labelled it the new oil, thanks to its ability to be monetised, some are now calling data the new asbestos due to the latent dangers of possessing it.

Recent high-profile events have shown that stolen data can be used for commercial gain. This includes information that could be used for identity fraud purposes, organisational secrets, details of pending transactions, sensitive personal information and information that is relevant to critical infrastructure or national security. Unlike other resources, though, the theft of data is not always obvious.

What's becoming clear is that we are seeing a new trend of data breaches at scale and the weaponisation of personal information against companies in possession of large databases containing personally identifiable information.

To protect against possible data breaches, organisations need to embark on classifying, organising and securing their information and data. In combination with digitising and unlocking value from data, we call this process 'information transformation'.

> Some are now calling data the new asbestos due to the latent dangers of possessing it.

Why prevention is better than cure

The impacts of a data breach on an organisation can be devastating. And not just financially.

In addition to the reputational risks, breaches can also negatively affect staff, shareholders, customers and partners. There is also the impact on stock values, potential lawsuits, dealing with APRA expectations and the unseen internal costs of managing the situation as it develops.

The global average cost of a data breach in March 2023 was USD $4.45 million[1] – a 15% increase over the past three years. In Australia, that figure is USD $2.7 million.[1]

But sensitive information isn't just being held by big corporations. There has been a massive increase in the amount of data that is now being collected and stored electronically across a broad range of industries and organisations, including small business. In fact, smaller organisations, those with 5,000 or fewer employees, saw an increase in the average cost of a data breach.[1]

Being able to prevent a data breach, or take action to minimise the impacts should one occur, can not only save your organisation millions of dollars in remediation expenses and potential lawsuits, but it can protect your reputation, maintain your brand integrity, retain trust with your customers, and shield your staff from reduced productivity and morale.

USD $4.45 million

Global average cost of a data breach in March 2023[1]

USD $2.7 million

Australian average cost of a data breach in March 2023[1]

A challenge on a global scale

Cyber risk is a challenge that all organisations face. A number of recent high-profile data breach cases in Australia served as a timely reminder that no organisation is immune.

Because of the damage that can occur with large scale data breaches, governments around the world are increasing penalties and legal regulation around information security.

Currently in Australia, all businesses with turnover in excess of $3 million are subject to the Commonwealth Privacy Act, which requires mandatory reporting of data breaches involving personal information.

However, in the wake of the recent breaches, the government announced it will increase penalties for serious and repeated breaches of the Privacy Act 1988 from $2.1 million up to $50 million, and that in the future the Privacy Act will apply to all organisations, including businesses with less than $3 million in revenue. That's an enormous concern for small businesses.

With this explosion in the legal impacts of cyber events, company directors and managers are becoming increasingly concerned about information security issues. Now more than ever, preventing a data breach is paramount, because once the damage is done, it often can't be undone.

But Australia isn't alone in its pursuit of managing cybercrime. According to Cybersecurity Ventures, the cost of cybercrime globally is estimated to reach USD10.5 trillion by 2025.[2]

Based on these numbers, if cybercrime were a country it would be the third biggest economy in the world after the US and China. It would lead to the biggest transfer of wealth in human history and would soon exceed the value of the international drugs trade for all major illicit drugs combined[2].

Knowing how to secure and protect information and data is critical and the penalties for getting it wrong can be significant.[3] But before you can secure and protect, you need to understand what data and information you have, the format it's in, why you have it and where it's stored.

Three key questions every organisation should ask

In a recent interview[4], Australian Institute of Company Directors CEO Mark Rigotti discussed the importance of building a company's cyber resilience. He referred to the advice of David Thodey, chair of Xero and Tyro Payments, in AICD's Essential Director Update last year that if you don't need the information or data you're holding, then get rid of it.

Mr Thodey also posed three essential questions that company directors should be asking:

1. **What data do we have that cybercriminals want?**
2. **Why do we have it?**
3. **Is it coded or encrypted?**

Understanding your data: structured vs unstructured

There are different types of data structures that encompass customers, clients and employees. Structured data includes generated and transactional information, such as a health record, financial transaction or a contract, as well as observed information.

Unstructured data covers an evolving range of sources such as the Internet of Things, video analytics, artificial intelligence and machine learning models.

It's in the unstructured domain, where we move from personal records to real-time information, that we're seeing the greatest shift.

In this space, large volumes of heritage data are being utilised in massive information sets. The challenge for organisations is how to manage that integration and trust the process.

More often than not, organisations and data grow in siloes so it's difficult to have a holistic view across the organisation. Trying to identify, categorise and manage data in this state is a tall ask.

By transforming unstructured information into structured data and digitising where relevant, you can meet your regulatory and compliance obligations across the lifecycle of your information.

The lifecycle of data

You need to look at data as a continuum—it has a lifecycle—and therefore needs to be maintained. From creation to storage and how organisations are federated and share data, there are four core domains organisations need to consider when it comes to understanding their data.

The four core domains:

1. **Is it transactional?**
2. **Is it evidentiary?**
3. **Does it have identity?**
4. **Does it require a lifecycle?**

If data has a lifecycle, for example needs to be stored or shared, how do you manage that? If you're dealing with a third-party, do they have the right security levels to handle your data? If you're replicating data across your organisation, is the process fragmented or is the data being captured and stored in a like-for-like way? What about the hierarchy for destruction or dispossession?

When every record has a digital identification, you can search and identify your structured records with ease, automate workflows to drive efficiencies and unlock valuable data insights to make better operational decisions.

> The data that an organisation holds suddenly becomes really important once it realises that it has been the subject of a data breach. Because one of the first questions management will want answered quickly is: what information do the hackers have?

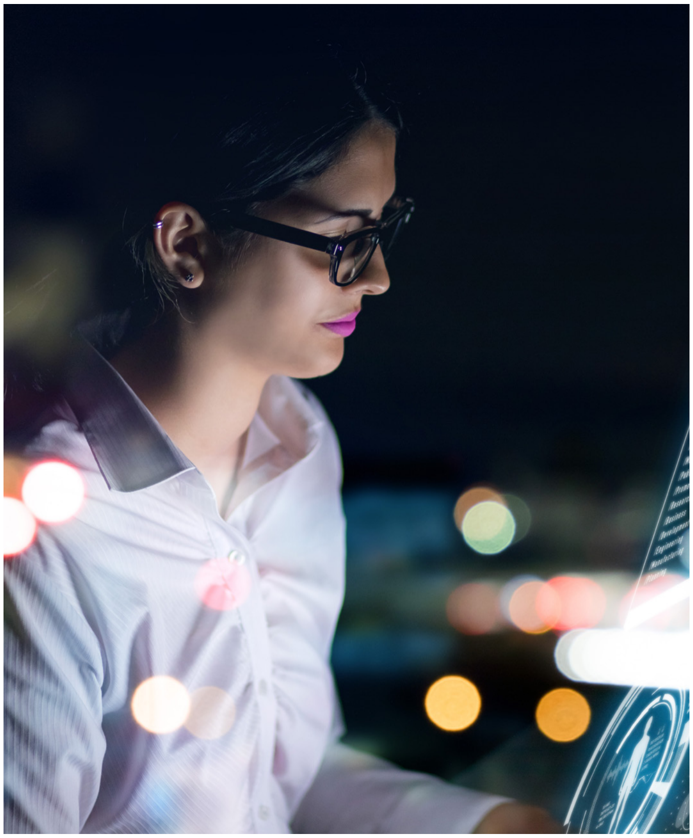
Preventing a breach by transforming your information

To avoid becoming one of tomorrow's headlines and to ensure your organisation is prepared to protect its customers and the company from reputational and financial damage, organisations need to move away from the 'keep everything' culture.

It cannot be stressed enough how important it is for an organisation to understand data risks and to introduce information governance across every department.

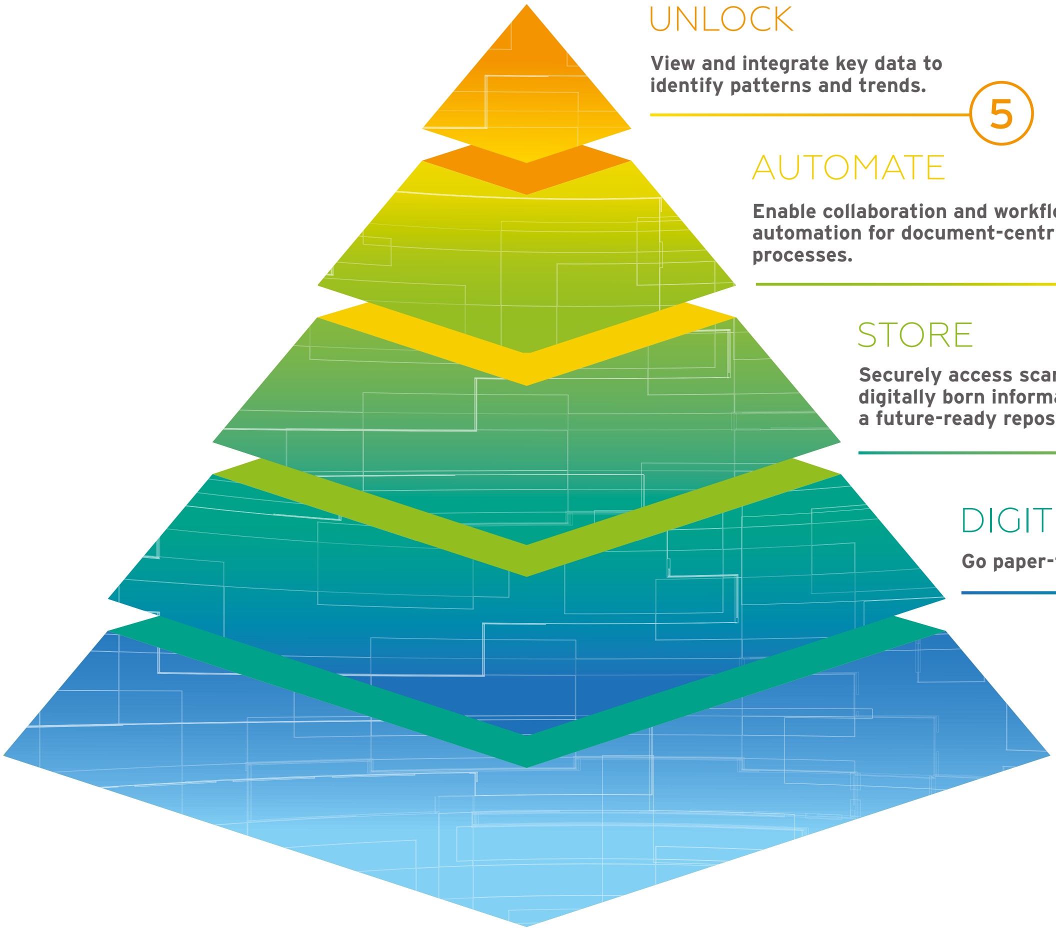
To protect against possible data breaches, organisations need to embark on organising, securing, digitising and unlocking value from their information and data.

We call this 'information transformation'.



A 5-step guide to transformation success

Having a transformation plan is key to modernising your data and information management processes. Here is a five-step process to achieving that.



UNLOCK

View and integrate key data to identify patterns and trends.

5

AUTOMATE

Enable collaboration and workflow automation for document-centric processes.

4

STORE

Securely access scanned or digitally born information from a future-ready repository.

3

DIGITISE

Go paper-free or paper-light

2

IDENTIFY

Determine what should be digitised, stored or defensibly destroyed

1

1. Identify

Determine what should be digitised, stored or defensibly destroyed.

You can't make good business decisions if you don't know what you have in your data and information inventory. Once you know what data and information you have, you need to understand your information governance regulation requirements and develop an information governance program and retention schedule so you can effectively manage your data and reduce risk.

2. Digitise

Go paper-free or paper-light.

Paper documents that are pertinent for business operations should be converted into digital format so they're easier to access and analyse. But not everything needs to be digitised. According to an Iron Mountain study, around 60% of documents are redundant, obsolete or trivial. To determine what to digitise, you need to understand your compliance requirements, the potential monetisation value of the data, whether you need to access it for business and/or audit needs, the cost of digitisation and storage, and the impact on existing processes, SLAs and people.

3. Store

Securely access scanned or digitally born information from a future-ready repository.

With a secure cloud storage repository, you can ingest documents from various locations, such as other cloud repositories, enterprise content management systems (ECMs) and file shares. By centralising your scanned and digitally born documents, you gain enhanced visibility, better connections and improved access.

4. Identify

Enable collaboration and workflow automation for document-centric processes.

Once your data and information has been sorted, you should look to automate manual processes where possible. A combination of digitalisation and modern technology that integrates with your existing systems can help eliminate bottlenecks and free up your employees to focus on more high-value tasks.

5. Unlock

View and integrate key data to identify patterns and trends.

Your final step is understanding your data and drawing insights. By aggregating and visually connecting your data through dashboards on one platform, you'll gain powerful insights to make more informed business decisions. It also has the potential to uncover new revenue streams you may not have considered before.

Additional Considerations

- **Executive sponsorship**
  To successfully transform your organisation's information, sponsorship needs to come from the top. By showing the business how the organisation will benefit from the change, the leadership team needs to show the organisation how it will benefit from the change and determine the key objectives and success metrics.

- **Building a cyber-aware culture**
  Managing the lifecycle of data –both physical and digital –isn't the job of one team. You need to create a cyber aware culture that encourages and empowers all staff across the organisation to be accountable and responsible for protecting data and information.

- **Instilling information governance at all levels**
  Developing an information governance framework allows you to define how your organisation creates, uses, shares, stores, archives, values and deletes physical and digital information. Introducing a well-defined retention schedule lets you identify how long important data and information needs to be retained before it can be destroyed. Doing so means you're better equipped to meet your legal, statutory and regulatory requirements and reduce risk.

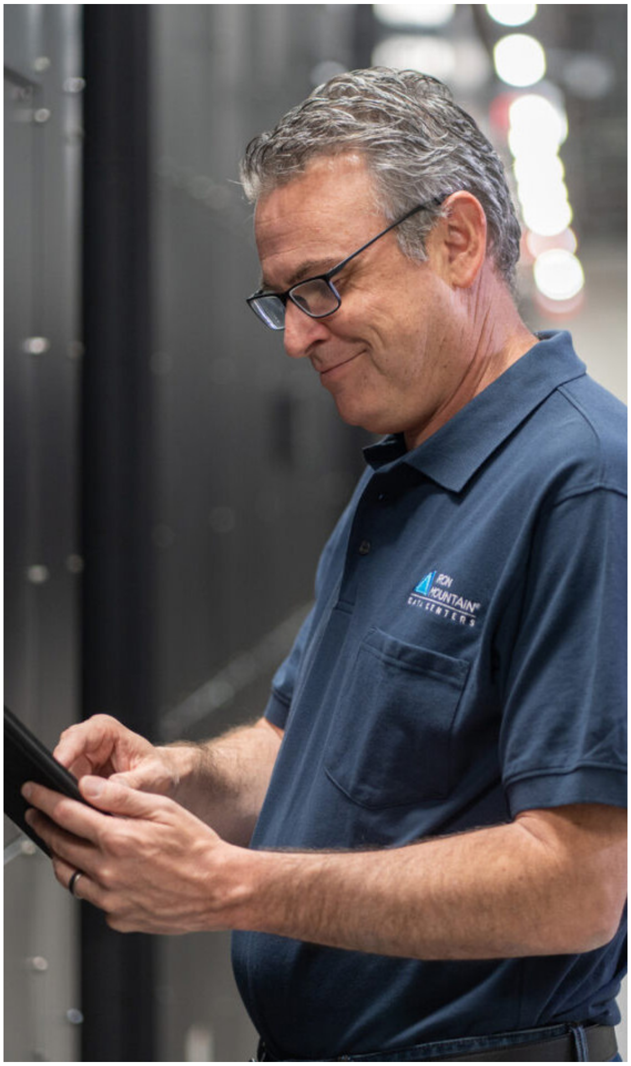
Conclusion

It’s imperative that business critical information and data is properly managed through its entire lifecycle.

Undergoing an information transformation, which involves organising, securing, digitising and unlocking value from your data and information is your best defence against a data breach.

Partnering with the experts in data and information lifecycle management means that your organisation can be better prepared, minimise risk, and be ready to respond to a data breach.

Iron Mountain has spent their lifetime supporting businesses to secure, protect and manage their information. Contact the team at Iron Mountain to gain expert guidance on how to transform your information and data.



Sources

[1] Cost of a Data Breach Report 2023, IBM Security

[2] Cybercrime to Cost the World $10.5 Trillion Annually By 2025, Cybercrime Magazine https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/

[3] More information on the legal impacts is available at: https://www.lawandcyber.com.au/insights

[4] Interview of Mark Rigotti by Kirsten Galliott in Qantas Travel Insider No.362, August 2023.

IRON MOUNTAIN®

& LAW CYBER

1300 476 668 | ironmountain.com/au
0800 723 255 | ironmountain.com/nz

contact@lawandcyber.com.au
lawandcyber.com.au

About Iron Mountain

Iron Mountain Incorporated (NYSE: IRM) is a global leader in innovative storage, asset lifecycle management, and information management services. With over 70 years of experience serving more than 95% of the Fortune 500 and 225,000 companies worldwide, Iron Mountain helps customers CLIMB HIGHER™ to transform their businesses. Through a range of services including digital transformation, data centres, secure records storage, information management, asset lifecycle management, secure destruction, and art storage and logistics, Iron Mountain helps businesses unlock value and intelligence from their stored digital and physical assets at speed and with security while supporting their sustainability goals.

About Law & Cyber

Law & Cyber provides cyber risk advisory services including in-person and online education, cyber incident tabletop exercises for executive teams, legal advice and consulting. Contact Law & Cyber for expert advice on building a cyber-aware culture in your organisation.

Simone Herbert-Lowe has educated more than 10,000 Australians about cyber risk through specialist online and face-to-face training that explains how cyber, legal and business risk intersect. With more than 30 years of experience in private and corporate legal practice, Simone specialises in supporting businesses' cyber resilience through education and fostering a cyber-aware culture. Simone regularly presents to businesses on cyber risk, facilitates cyber incident tabletop exercises, and has given expert written opinion in legal proceedings. Simone's outstanding leadership was recognised with AGSM's Wanbil Lee Prize for Ethical Leadership in Business in 2016 and the Innovator of the Year (Individual) Award at the Lawyers Weekly Women in Law Awards in 2022.