



KONICA MINOLTA

# The value of your information and how to secure it

## Key Findings

- Managing and protecting information is an ongoing challenge and a major, increasing business expense.
- Significant indirect costs are often overlooked when determining the true cost of data breaches, most of which are a result of activities within the organisation.
- These costs are mostly incurred as a result of activities within the organisations themselves.
- The security of hardcopy information and digitising of document-based processes are critical to the success of an enterprise-wide data security policy.

This article reviews recent global research uncovering the significant value organisations place on their information, and detailing both the direct and indirect costs associated with breaches in information security. It also highlights some of the key findings, provides analysis of our own local research, assesses the implications for Australian organisations and outlines best practices for managing valuable information.

## The real value of information

Depending on your industry sector, the information that your organisation owns could account for the majority of its total value.

Loss or exposure of valuable data could significantly harm your organisation. When asked about potential damage to their business in a recent global survey<sup>1</sup>, 49% of respondents predicted lost customers as the main consequence of losing business information and 47% indicated their brand would be damaged as a consequence of losing business information. This was higher than the 41% of respondents predicting decreased revenues and 39% increased expenses.

Other potential costs can include fines for breaching consumer or privacy legislation, or civil action. There is therefore a growing need to effectively manage information and mitigate information security risks.

Managing all this information is costly for Australian businesses of all sizes. As electronic information is more readily available and heavily relied upon in all areas of the business, organisations become more reliant upon the management of their data and information systems. The modern day organisation must therefore embrace the challenge of managing and improving their information systems and securing their data.

<sup>1</sup> *State of Information 2012*, conducted by ReRez Research on behalf of Symantec Corporation with 4,506 IT professionals from global organisations in 36 countries

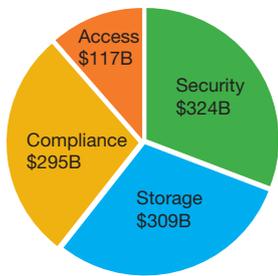
<sup>2</sup> *Document & Data Security Study*, conducted by Woolcott Research for Konica Minolta with senior decision-makers from 262 small-to-medium Australian businesses in late 2012



### Assessing the value of information

Information is estimated at 49% of the average organisation's total value. Despite its importance, IT executives still face challenges: 69% reported loss of important business information and 69% experienced exposure of confidential information. One in three had regulatory compliance issues relating to information.

Worldwide spending on business information is believed to be US\$1.1 trillion, comprising:



Source: State of Information 2012, ReRez Research on behalf of Symantec Corporation, March 2012

## Australian attitudes to document and data security

Konica Minolta recently commissioned an Australia-wide study on document and data security<sup>2</sup> with senior decision makers of small-to-medium businesses. Key findings of the research delivered both good and bad news about their understanding of information risks and the actions they took to mitigate them. The following table illustrates these findings:

94% of Australian businesses are aware of security risks in their own organisation but...	Only 25% are taking the issue seriously by addressing it directly with staff
98% believe their security processes are effective in safeguarding their documents but...	60% say they are still concerned about document security risks 76% don't believe an office printer is a potential security risk 13% admitted to finding confidential business intellectual property on a printer Only 25% of businesses have security pin codes on their output devices
60% have a security policy to govern the use of mobile devices when accessing company data, but...	58% were unaware documents could be printed from smartphones using a printing application
84% of businesses have an archival recovery plan, but...	46% believe their archival system is at risk of fire or theft

Our research suggests that security gaps remain. Despite the fact Australian enterprises value information security, and are aware of their exposure to document security risks, there are significant opportunities for further minimising information security risks.

Proper configuration and management of print output devices, for example, can mitigate document security risks. These devices can be customised to manage the flow of information within an organisation to meet specific risk profiles and information security policies.

## The true cost of data breaches

It is important to consider direct and indirect costs when calculating the true cost of data breaches. When these associated costs are accurately identified, the results can be eye-opening. According to Ponemon Institute research<sup>3</sup> across the US, EU, India, Japan and Australia in early 2012, the average total organisational cost of data breach in Australia was US\$2,270,862.

Of the Australian organisations participating in the research:

- The most significant cost was 'Lost Business', with \$879,557 on average per breach.

<sup>3</sup> 2011 Global Cost of Data Breach, conducted by Ponemon Institute for Symantec Corporation in early 2012 with IT, compliance and information security practitioners with 209 global organisations including 22 from Australia



---

## Mitigating risks

In terms of mitigating risks of data breach, Australia was the third most likely (at 41%) to centralise data protection and appoint a security professional to C-Level, just behind the US and UK (43% and 42% respectively). This indicates that Australian organisations are not alone when it comes to failing to establish a formal centralised structure that mitigates information security risks.

**Source:** 2011 *Global Cost of Data Breach*, conducted by Ponemon Institute for Symantec Corporation in early 2012 with IT, compliance and information security practitioners with 209 global organisations including 22 from Australia

---

- The cost of detecting and escalating a data breach was calculated at an average of \$812,137, while estimated costs incurred after a data breach averaged \$499,218.
- The estimated per capita cost of each data breach was \$145, of which only \$58 represented direct costs. The greater proportion of costs was attributed to indirect costs to the organisation; such as the time, efforts and internal resources spent on investigation and remediation.
- 32% of data breaches were caused by the carelessness of insiders; the same percentage was attributed to system glitches and nearly as high as breaches caused by 'malicious' intentions (36%).
- Half of the Australian organisations surveyed experienced a data breach for the first time in 2011, indicating breaches are on the rise.
- After suffering a breach, 41% needed to engage external consultants to help remedy the situation.

Australian organisations are therefore greatly affected by a growing number of data breaches, the causes of which mostly stem from within their very organisation.

## Three approaches to mitigating information security risk

Given the value of your organisation's information, developing policies and best practices for its management and protection is essential.

Having surveyed 4,506 IT professionals from around the world<sup>4</sup>, Symantec formulated a series of recommendations for how organisations can become more 'information-centric' to better protect their valuable data. According to the research, the three overarching approaches to overall data security policies, processes and behaviours are:

### 1. Focus on the information itself, not the device or data centre

Symantec recommends the first step is to focus on building an information infrastructure that optimises the ability of staff to find, access and consume critical business information, regardless of location or method.

Relating this to your own business environment, further considerations might also include:

- **Where your data is stored:** for example, is your data stored on or off-site, in a data centre or the cloud within Australia or offshore?
- **How your data is stored:** for example, is your data stored as a hardcopy or is it stored digitally. Is it backed up to physical or electronic archives, or are you replicating live data?
- **The applications that access it:** for example, which business processes and workflows are drawing on which data sources? Furthermore, what level of security do these applications have?
- **Devices used to access and display it:** for example, are the devices used to access and display the data company-owned or BYOD, and are they computer or mobile devices?

---

<sup>4</sup> *State of Information 2012*, ReRez Research on behalf of Symantec Corporation, March 2012



---

## How Managed Print Services (MPS) can increase information security

A recent Quocirca<sup>5</sup> survey of mid-sized businesses across Europe found that 46% want to enforce a print policy and 41% are concerned with document security. This research uncovered that poor document security was impacting employee productivity to much the same degree as toner availability. It was also found that improving information security was a strong contributing factor when adopting a Managed Print Service (MPS), in addition to other associated benefits of MPS; namely print tracking and cost recovery.

An experienced MPS provider can improve your information security by ensuring that your organisation's print output devices and document management processes achieve a desired level of information security and comply with existing information security policies.

A customised program can be built to address specific information security requirements and address information security issues through important, often overlooked activities, such as hard drive encryption, auto-deletion, pull printing, print log-in, report audit trails and document storage.

### 2. Not all information is equal

It is critical to gain an understanding of your information, including who owns it and whether it is personal (such as wage or employment records) or business (sales records or intellectual property, for example). This is because complete visibility over your data will enable you to accurately map and classify it to discover its relative value, enabling you to then prioritise security, protection and management for the information that matters most.

### 3. Be consistent

Set consistent policies for your information wherever it is located in physical, virtual or cloud environments. This will unify information classification, enable automated discovery of who owns and uses specific information, and result in reliably consistent access and distribution controls. Inconsistency in the ways you treat data creates more work in managing it, and can introduce vulnerabilities into your overall information security policy.

Adopting these three approaches and integrating them into your organisation creates the foundation for adequately valuing the information assets of an organisation, and developing a comprehensive information security framework.

## Summary

The statistics gathered by recent leading global research indicate that:

- A large proportion of an organisation's value is attributed to its information assets.
- The cost of a data breach not only encompasses direct costs such as lost revenues, data recovery and the costs of system remediation (often calling for support from external consultants), but is also likely to incur significantly greater longer-term indirect costs such as loss of business and damage to your reputation with customers and the market.
- While most business decision-makers now have a good understanding of the potential risks, there are areas which need more attention in regards to securing corporate data.

A series of approaches that make your organisation more 'information-centric' will enhance information security. The formulation of appropriate enterprise policies for protecting data will also provide a sound foundation for securing the valuable information your organisation is reliant upon. When these policies are complemented by the adoption of best practices for managing and processing information, the highly valuable information of an organisation will not only be better protected, but flow-on effects for staff productivity and greater speed to market will also be realised.

A vital consideration when approaching the task of information security is to determine effective solutions for the management of hard copy information within your organisation. This is where the security expertise and experience of an MPS provider can offer significant and measurable benefits.

---

<sup>5</sup> *Managed Print Services: An SMB Priority*, conducted with 500 European businesses with 50-500 users by Quocirca in 2011