insight
QRMC NEWSLETTER
QRMC
Risk Management

Issue 51 November 2014

Insight aims to provide useful information, links and tips in the areas of Risk Management, Occupational Health and Safety, Business Continuity Management, and other areas relating to management systems and corporate governance.

This issue:

- Business continuity and data management
- Holiday wishes

Business Continuity and Data Management

Operating in the fast-paced, interconnected and well-regulated modern world, organisations are more reliant than ever on the accuracy, completeness and security of the data which are collected and generated as part of their business operations.

As highlighted by advice distributed prior to the recent G20 meeting in Brisbane, organisations are vulnerable to the loss of, or damage to, stored digital information.

As the quantity of information generated and kept continues to rise, and at the same time the easy and real-time access to data by employees on- and off-site becomes more critical to business operations, the management and storage strategies for this information becomes vital.

Each organisation needs to consider the management and storage of data for their own needs and within their own operational context as part of good business continuity and organisational resilience planning. Not all organisations will find utility from the same data management tools and strategies.

However, some basic principles apply for all organisations:

1. Understand what information you have and need

It is easy for each officer or employee of an organisation to go about their business of fulfilling their daily duties without anyone in the organisation gaining a complete overview of the information required to keep the organisation functioning well. It is important to conduct this internal research, and then make informed decisions about how quickly

each set of data would need to be recovered if disrupted, how long it needs to be retained after storage, how secure it needs to be etc.

2. **Consider compliance implications**

   No industry is entirely without regulation; some industries are very highly regulated. Without explicit knowledge of the information required for the organisation to maintain compliance with the relevant legislative requirements, it is possible to slip into a state of non-compliance through ignorance or negligence.

3. **Make determinations about what to keep and for how long**

   Some data needs to be kept for a specific number of years, and some data must be kept indefinitely whilst the organisation is operational. This should be checked and documented in a data retention policy.

4. **Decide on a hierarchical prioritisation**

   Some information will be an absolute prerequisite for critical organisational functions. Other information may be important, but can be done without for a period of time. Ensure that fast storage/backup and restoration hardware and processes are in place for the former over the cheaper archival and restoration options for the latter.

5. **Understand storage options**

   Many organisations are heavily reliant on cloud-based backup options. There are still plenty of local network and hardware based options in use as well, not to mention good old hard copy. Carefully research the pros and cons of all options open to the organisation, including the various types of cloud-based services which are by no means exactly comparable, and ensure the optimum choice or mix of alternatives is chosen.

6. **Scrutinise providers**

   If hard copy archival providers are expected to provide safe, environmentally controlled, fire-retardant spaces to keep hard copy information safe, the same level of expectations and scrutiny should apply to providers of electronic storage services. Check everything from security to technical and accounts support to ensure your data is safe and that you'll have the assistance you need in the event of a business disruption.

7. **Be certain of security**

   Rather than simply relying on the cloud provider's systems or your local firewalls and virus protection protocols, ensure critical and/or confidential information is encrypted as a matter of course, so that if it is hacked or stolen from your own network or the cloud, it remains secure.

8. **Minimise superfluousness**

   Redundancy is a keystone to business continuity and disaster recovery, however data which is truly surplus to requirements just wastes resources in managing it. Check if you are storing any information which is in fact useless to the organisation, and either move it to the lowest rung on the archival ladder or remove it completely.

9. **Check access**

   Many people remember backup protocols which resulted in a completely unintelligible compressed file, inaccessible unless the exact hardware and software was available to translate it, which was not always the case in a severe business disruption event. While backup options have become much more user-friendly than this, accessibility should be checked – if you can't find and restore specific bits of critical stored data quickly and easily, your data management processes are worthless.

10. **Test reliability**

    Assuming your data collection, storage, backup and restoration processes are working, and then suffering a disruption and finding out they were not working after all, is a terrible experience. Test and check and be confident.

Please contact QRMC for more information.

Holiday Wishes

This edition of *Insight* is the final for 2014. The first edition in the new year will be issued in February 2015.

QRMC Risk Management Pty Ltd will be closing over the Christmas period, from close of business Friday 19 December, reopening Monday 5 January 2015.

QRMC wishes all our clients, supporters and readers a relaxing and happy holiday season. Take care and stay safe until we meet again in the New Year!

The material contained in this publication is in the nature of general comment only and neither purports, nor is intended, to be advice on any particular matter. No reader should act on the basis of any matter contained in this publication without considering and, if necessary, taking appropriate professional advice regarding their own particular circumstances.