LexisNexis

Internet Law Bulletin

2018 . Vol 20 No 9

Contents

Information contained in this newsletter is current as at February 2018

LexisNexis Butterworths

Business continuity — it pays to have a plan

Ian Bloomfield *IGNITE SYSTEMS*

In the legal system time stops for no one, court dates are fixed (not chosen), contracts have deadlines and clients expect to see their matter progressed. Therefore, any disruption to doing business is a huge risk to a law firm. As a lawyer representing a client on a matter, you have a fixed timeframe to build your case, do the research and so on. If you find yourself unable to complete your preparation just days before court, it could be detrimental to the outcome of a case, with potentially serious professional ramifications.

Business continuity is about identifying potential threats to the normal operation of your firm and having arrangements in place that enables a response so you can keep doing business with as little disruption as possible.

This article discusses business continuity, its importance for law firms and how you can go about creating a business continuity plan for your law firm.

Takeaways

- It is given that good governance is an essential requirement for every law firm and business continuity should form part of the governance framework as an element of risk management.
- Business continuity and disaster recovery are not the same thing. Both have to do with business preparedness, but whereas disaster recovery is tactical, business continuity has a strategic focus.
- For any given law firm, there are many unpredictable and uncontrollable scenarios that could disrupt their normal operations.
- Creating a business continuity plan does not have to involve a complicated process but engaging a suitably qualified service provider will greatly assist in preparing and maintaining a business continuity plan.

What is business continuity?

A business continuity plan involves planning and preparing for how your firm can continue to operate after an unplanned but credible event disrupts normal arrangements, processes, systems or services. It sets out a framework for an effective response following such a disruption, in order to return to "business as usual" in the quickest possible time.

Business continuity has to be considered in the context of an organisation's overall approach to risk management and as such it should form part of an organisation's governance framework. There are a number of articles by the Governance Institute of Australia (GIA) that highlight the nexus between business continuity, risk management and governance.[1]

Business continuity also features as an important element of privacy governance. The guidelines published by the Victorian Commissioner for Privacy and Data Protection state that "business continuity management should feature as a key component of a security management framework".[2] The Office of the Australian Information Commissioner (OAIC) in its *Guide to Securing Personal Information*[3] asks "do governance arrangements include risk management and business continuity plans?"[4]

It should be noted that a business continuity plan is different from a disaster recovery plan, though the latter forms part of a business continuity plan. A disaster recovery plan only focuses on getting specific systems up and running after a disaster, typically involving restoration of IT infrastructure or recovering data.

What are the benefits?

Some of the many benefits include:

- Good governance — having a business continuity plan is an essential component of good governance.
- Quick and effective response to a disruption event — proactively identifying the potential events and impacts for likely scenarios and establishing an effective response plan makes it possible to react quickly and promotes good decision-making.
- Reduced risk of financial loss — when a business is unable to operate, it has a direct impact on the ability to generate revenue.
- Mitigate reputational damage — maintenance of a law firm's brand and image is dependent on its ability to service clients and work effectively with associated law firms. Minimising any impact from a disruption event avoids any erosion of confidence.
- Meet legal and statutory obligations — the ability to meet legal and statutory obligations could be

put at risk if a law firm is unable to continue operating effectively as a result of a disruption event.

What are the risks?

Most law firm principles are unlikely to have any firsthand experience with events that disrupt the normal operations of their firm. This lack of past experience can make it difficult to consider business disruption as a tangible risk. As a result, it is easy to see how business continuity planning is often a low priority.

Contrast this with how people view the need for insurance to cover natural disaster events such as fire and flood, or to cover theft or the need for professional indemnity. Even though most have not had experience with these events, nevertheless they are considered a possibility with the potential for catastrophic consequences thereby justifying the need for insurance.

Let's look at the types of scenarios that could disrupt the normal operations of a law firm.

Cyber incident

Barely a week passes without the announcement of a significant cybersecurity incident. The diverse impact of these events reinforces the fact that every law firm is dependent on digital business capabilities. A cybersecurity incident is a real and present danger to the operations of every law firm. There are countless stories of law firms being out of action for 1 or more days as a result of a ransomware attack or something similar — the recent DLA Piper incident being a case in point.

Fire

A fire is a risk that every law firm faces and it is completely unpredictable, but nevertheless a possibility. The damage from a quite small fire, depending on its location, could still make an office unusable or seriously restrict normal operations. In addition, there is the impact of smoke and water damage. A worst-case scenario would be an office that is seriously damaged or destroyed by fire, requiring an alternative work location for weeks or even months.

Flood

Flood, or more generally, water damage is a natural disaster risk faced by most suburban and regional law firms. It need not be a flood situation, as the damage from water ingress resulting from a severe storm can be just as damaging. Even a city law firm located in a multi-storey building faces the risk of a building services failure that could lead to serious water damage — think about the accidental operation of fire sprinklers.

Essential services

Water, electricity or sewerage are things that every law firm office requires in order to remain operational. The loss of any one of these essential services is not completely beyond the bounds of possibility, but it is completely unpredictable.

Environment

There is a huge range of environment scenarios that could leave a law firm unable to access their offices. Some of these include:

- building damage or instability making its occupation unsafe
- a gas leak in the vicinity causing an area to be cordoned off
- action by police to restrict access to an area in order to contain or respond to a situation
- an airborne hazard resulting from a chemical spill or a fire involving hazardous materials

Staff

The importance of staff should never be overlooked. The loss of a key staff member due to illness or accident could mean operating without valuable knowledge, special skills or even an essential certification. This has the potential to seriously impact the operations of a law firm.

Infrastructure

The loss of critical infrastructure can occur for a wide range of reasons including:

- failure of equipment
- failure of software systems
- failure of virtual systems in the cloud

Business services

The main business services with the potential to wreak havoc on a law firm are internet access and telephone services. Loss of internet could result from a service provider issue, think of all the recent stories about the National Broadband Network (NBN) service problems or something as basic as a cable being dug up in the street. For many law firms today, their telephone service is dependent on having an internet service and for those with a traditional telephone service, it could be out of action for days because of a fire, flood or equipment failure at an exchange.

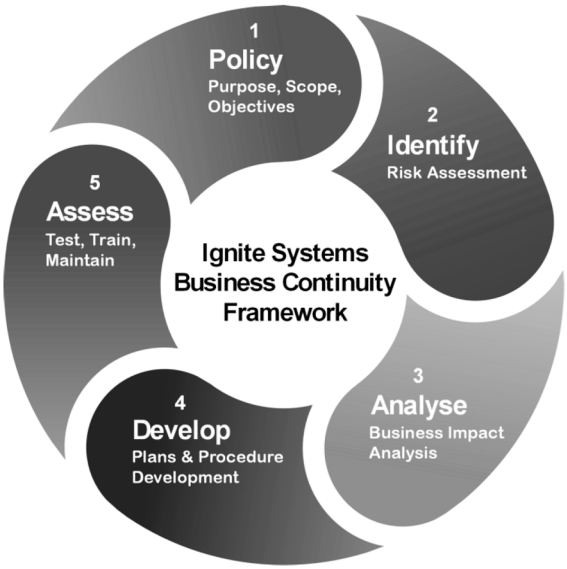
This is not an extensive list of scenarios but these examples serve to highlight the broad range of situations, mostly unpredictable and uncontrollable, that could disrupt the normal operations of a firm.

Creating a business continuity plan

Before embarking on the creation of a business continuity plan, it is important for an organisation to understand that managing risk has to be recognised as a strategic priority in order to support business continuity. For many law firms, this is a significant step because traditionally business continuity has been seen as an IT function and not an organisation-wide risk.

There are many good guides and templates to assist with the creation of a business continuity plan. Organisations that make these available include the GIA and many other government bodies.[5]

The process of creating a business continuity plan does not have to be complicated. Outlined below is a relatively simple framework that I recommend for small to medium law firms.



Step 1: policy — purpose, scope, objectives

Create a policy that sets out what the purpose of the business continuity plan is, the scope of the plan and what the intended results of the plan are. This should articulate the main elements of the plan and it should include details of the roles and responsibilities that are essential to the development, execution and maintenance of the plan. It is important that the policy is concise and easily understood so that all staff and stakeholders are able to assimilate its essence.

Step 2: identify — risk assessment

A risk assessment is the foundation on which a business continuity plan is built. It identifies, quantifies and qualifies the risks a law firm is exposed to and it informs almost all other decisions made in the process. It involves identifying and analysing credible scenarios that are likely to have an adverse effect on your ability to conduct business. These scenarios are then prioritised according to their likelihood and impact, then methods of dealing with each one is developed in the form of preventative actions and contingency plans.

Step 3: analyse — business impact analysis

This step involves identification of critical business functions and determination of how long your firm could survive without performing each of these functions. This determines the recovery time objectives (RTO) for each function. The RTO is the time from the onset of a crisis/disaster to the time that the critical business function must be fully operational in order to meet your business continuity objectives. Having identified the RTOs, it is then possible to establish the timeframes applicable to the various contingency plans.

Step 4: develop — plans and procedure development

With the completion of the assessment and analysis, it is then possible to develop detailed plans and procedures to enable execution of the various contingency plans. This should include disaster recovery plans for specific IT systems. It is important to make sure roles and responsibilities specific to the execution and maintenance of the plans and procedures are documented.

Step 5: assess — test, train, maintain

It is essential to understand if your plan meets the objectives set out in the business continuity policy and is therefore fit for purpose. Testing a business continuity plan, sometimes called exercising, involves working through a potential disruption scenario and considering how your plan would be applied in that situation. This will enable identification of areas for improvement so that you can modify your plan accordingly. The process of exercising is also an excellent way to provide training to staff so that they are prepared if the real thing occurs.

When testing your plan, it is important to consider the role of any third parties you intend to rely on.

Maintaining a business continuity plan involves a scheduled process of review to ensure that everything is up to date, appropriate arrangements are still in place and documents are being managed.

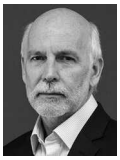
Conclusion

Every law firm needs to be prepared for the worst. Few firms can afford to be out of action for any period of time and the importance of a business continuity plan in relation to governance cannot be overstated. Building business continuity into your business culture and making it part of the way that you run your firm helps prepare you to deal with the unexpected and return to business as usual in the quickest possible time.

A business continuity plan will help you to:

- identify and objectively assess the risks
- act to reduce risks where possible
- prepare contingencies for risks that you can't control
- respond effectively if an incident or crisis occurs
- recover from an incident in a timely manner

Engaging a service provider that has an understanding of law firms and proven experience with business continuity, risk assessment and cybersecurity will greatly assist in preparing and maintaining a business continuity plan which is relevant to the way you operate.



Ian Bloomfield
Managing Director
Ignite Systems
ian.bloomfield@ignite.com.au
www.ignite.com.au

Footnotes

1. See for example GIA "Business continuity standard AS/NZS 5050 — links with risk management" available at www.governanceinstitute.com.au.
2. Commissioner for Privacy and Data Protection *Guidelines to Protecting the Security of Personal Information: 'Reasonable Steps' under Information Privacy Principle 4.1* (January 2017) www.cpdp.vic.gov.au/images/content/pdf/privacy_guidelines/IPP_4_Guidelines.pdf.
3. OAIC *Guide to Securing Personal Information: 'Reasonable Steps' to Protect Personal Information* (January 2015) www.oaic.gov.au/resources/agencies-and-organisations/guides/guide-to-securing-personal-information.pdf.
4. Above, at 18.
5. Guidelines and templates for creating a business continuity plan: GIA, Business survival — are you ready? available at www.governanceinstitute.com.au; Australian Government, When things don't go to plan, 31 January 2018, www.business.gov.au/new-to-business-essentials/series-two/when-things-dont-go-to-plan#whats-in-a-business-continuity-plan; South Australian Government, Protect your business, 28 November 2017, https://statedevelopment.sa.gov.au/industry/smallbusiness/business-continuity-planning; Queensland Government, Business continuity planning, 28 June 2016, www.business.qld.gov.au/running-business/protecting-business/risk-management/continuity-planning; UK National Counter Terrorism Security Office, London First and Business Continuity Institute *Expecting the Unexpected: Business Continuity in an Uncertain World* (2003) www.gov.uk/government/uploads/system/uploads/attachment_data/file/376381/Expecting_the_Unexpected_Reviewed.pdf; US Department of Homeland Security, Business continuity plan, 2011, www.ready.gov/business/implementation/continuity.