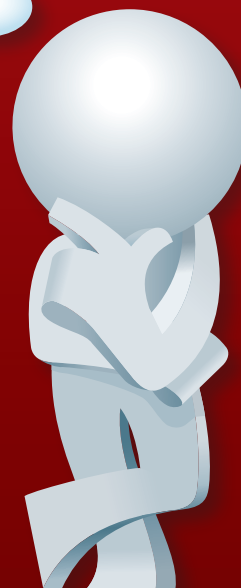




Australian Government

ORGANISATIONAL RESILIENCE



POSITION PAPER
FOR CRITICAL INFRASTRUCTURE

AUSTRALIAN
CASE STUDIES



ISBN: 978-1-921725-62-3

© Commonwealth of Australia 2011

This work is copyright. Apart from any use as permitted under the Copyright Act 1968, no part may be reproduced by any process without prior written permission from the Commonwealth. Requests and inquiries concerning reproduction and rights should be addressed to the Commonwealth Copyright Administration, Attorney-General's Department, 3-5 National Circuit, Barton ACT 2600 or posted at www.ag.gov.au/cca

Ministerial foreword



*The Hon Robert McClelland
MP Attorney-General*

Business plays a crucial role in Australia's social and economic wellbeing. Critical infrastructure organisations play an especially important role in providing essential services to other businesses, governments, and the community.

But there are a range of threats or hazards, such as natural disasters and equipment failure, which can disrupt or disable business operations.

So what happens when a business is disabled for a length of time? What are the impacts on its profitability, service delivery, and employees? What are the flow-on effects to the broader community? What are the key attributes that can help a business to bounce back or bounce forward from a disruption?

The Australian Government's Critical Infrastructure Resilience Strategy has identified a need to develop and promote a common understanding of, and body of knowledge about, organisational resilience. This booklet is one of a number of initiatives that helps to meet this need.

Organisational resilience: A position paper for critical infrastructure has been developed by the Resilience Expert Advisory Group (REAG) of the Trusted Information Sharing Network for Critical Infrastructure Resilience.

It provides a set of core resilience principles and attributes for critical infrastructure organisations, as well as general guidance on a methodology for organisations to consider and implement as appropriate.

Of course, resilience is not only important for critical infrastructure businesses that provide essential services to the Australian community, it's important for all Australian businesses. Our society is becoming increasingly complex and interdependent, which means we are all becoming more vulnerable to disruptive events.

That's why this booklet also provides a range of *Australian case studies* which illustrate disruptions to business operations, how the business dealt with the situation, and what lessons were learnt. Importantly, these real life examples help demonstrate some of the behavioural attributes that contribute to resilience.

I encourage all business owners to read this booklet – not only to help boost your resilience, which will help maintain your competitive edge and profitability – but also to help create a more resilient society.

REAG foreword

Many organisations are realising that traditional corporate strategies are not protecting them from an unexpected event. Organisations need to be resilient, they need to be able to absorb an event that necessitates change, to adapt and continue to maintain their competitive edge and profitability.

The viability and sustainability of organisations continues to be tested in a world that is constantly changing and with such changes come a range of new threats and challenges. Critical infrastructure systems and networks, in particular, are increasingly complex and challenged by a global operating environment of growing complexity.

The concept of organisational resilience for critical infrastructure is therefore both timely and important. For many critical infrastructure owners and operators the imperative to be resilient is high, as they need to ensure the continuity of essential services to other businesses, governments and the community in the face of all hazards.

An organisational resilience approach assists owners and operators to manage unforeseen or unexpected risks, i.e. those risks that, while plausible, might never have been experienced by an organisation before, are not categorised as foreseeable, and are not part of formal risk management processes or business continuity exercises.

Attributes of organisational resilience need to be better understood and integrated into an organisation's everyday life, philosophy and culture, which will ultimately help ensure survival in times of adversity. While organisational resilience means different things to different people, this paper seeks to set out a set of core resilience principles and attributes for critical infrastructure organisations, as well as a foundation for the tailoring of these attributes for organisations to consider and implement as appropriate.

John Valastro
Co-Chair
Resilience Expert Advisory Group

Organisational resilience: A position paper for critical infrastructure

Contents

Background	4
Purpose	5
Context	6
Resilience in the context of critical infrastructure	8
Benefits of a resilience approach	9
Principles of organisational resilience in critical infrastructure	13
Resilience – behavioural attributes	14
Leadership and culture	14
Networks	14
Change ready	15
Next steps	16
References	17
Acknowledgements	18

Background

On 4 December 2008, the Prime Minister delivered Australia's inaugural National Security Statement to Parliament, which included “preserving a cohesive and resilient society and strong economy” as one of five enduring national security objectives.

Following this, the Council of Australian Governments (COAG) agreed on 7 December 2009 to adopt a whole-of-nation resilience based approach to disaster management. The approach recognises that a national, coordinated and cooperative effort is required to enhance Australia's capacity to withstand and recover from emergencies and disasters.¹

Importantly, COAG recognised that disaster resilience will be strengthened where communities have continued access to essential services provided by critical infrastructure organisations.

On 30 June 2010 the Attorney-General launched the Australian Government's *Critical Infrastructure Resilience Strategy* and announced the establishment of the Resilience Expert Advisory Group (REAG).

The REAG had previously operated as the Resilience Community of Interest under the Trusted Information Sharing Network (TISN) for Critical Infrastructure Protection and contributed to two resilience workshops held at the Australian Emergency Management Institute (AEMI), Mount Macedon. The outcomes from these workshops have contributed to this paper.

The REAG's work program includes several initiatives identified in the Critical Infrastructure Resilience Strategy. The membership of the REAG is drawn from academia, business and government.

¹ COAG adopted the National Strategy for Disaster Resilience on 13 February 2011

Purpose

This paper has three objectives:

1. to outline the REAG's current thinking on organisational resilience
2. to share this thinking with the broader critical infrastructure community, including all levels of government and private sector organisations. The information in this paper may be relevant to resilience practitioners such as strategic planners, risk, security, business continuity and emergency managers, executive/general managers, regulators, policy makers, industry associations and insurers, and
3. to raise awareness of the need for an organisational resilience approach and to promote thinking on the concepts underpinning organisational resilience in the critical infrastructure community.

This paper details a set of core principles and resilience attributes that can be applied across a diverse range of critical infrastructure organisations. This information will also inform the development of a number of REAG initiatives, including a resilience maturity model. Once the model is completed, individual organisations will be able to assess their resilience maturity, develop their own specific strategies, and make informed decisions on allocating resources in the face of potential disruptions.

Context

The concept of ‘resilience’ is becoming increasingly popular. This stems from growing concerns about the need to manage uncertainty in modern societies and economies that are complex and vastly interconnected. Applying the concept of resilience to the fundamental elements of infrastructure on which our society and economy depends, is important for ensuring Australia’s ongoing economic prosperity and social wellbeing.

The term resilience is used in a broad range of contexts including – individual, community, ecological and organisational resilience. As such, definitions of resilience have evolved in parallel with many different interpretations and understandings. With respect to organisational resilience, emerging ideas involve ways of assisting organisations to effectively manage adverse/disruptive situations and capture or realise any presenting opportunities.

Resilience is not a one off program or a management system that can be developed and then reviewed annually or as required. It is an approach that takes time to develop and as indicated in this paper, is not one size fits all.

In responding to any potential barriers such as expense, engagement or cultural change, it is important to note that the elements of a resilient organisation are all fundamental to an effective and efficient business that is cognisant of risk, strategic planning and contingency based management. Further, a resilient organisation’s objectives and strategies will not conflict with its overall business goals but will complement them.

The nature of the challenges critical infrastructure organisations encounter means that applying the concept of resilience is not simple. There is demand for clarity or at least consistency in advice on applying the concept of resilience. Providing this clarity will ensure critical infrastructure organisations continue to develop the optimum capacity and capability for delivering their objectives in uncertain and non-routine environments.

The context in which critical infrastructure organisations operate includes challenges such as rapidly changing operating environments, and reliance on highly interdependent systems and globally dispersed third party providers.

This paper does not therefore propose a single pathway or specific tactical response to promoting resilience. Instead, it proposes a generic set of resilience principles and attributes for critical infrastructure organisations, and a foundation for an individualised methodology for organisations to consider and implement as appropriate.

As all organisations face unique risk landscapes, a one size fits all guide would be inadequate. Rather, resilience is seen as an outcome and a fundamental part of the governance of an organisation. The resilience outcome is therefore achieved through the contribution of a wide range of disciplines.

Organisational resilience results from a combination of what is considered traditional/technical (hard) and organisational/behavioural (soft) elements. This mix varies with the nature, objectives and culture of the particular organisation.

The importance of assets and financial management to organisational resilience is recognised. This paper is not, however, aimed at those responsible for designing infrastructure to achieve the outcomes of reliability, redundancy and robustness. Similarly, financial resilience is beyond this paper's scope. It is recognised that there are already a number of existing management systems that address uncertainty and unknowns within the areas of asset management and financial systems.

It is also recognised that approaches such as Total Quality Management and Business Excellence have been developed to ensure quality outcomes in routine and consistent operating environments. Also, while sustainability focuses on the long term performance of an entity, resilience is focused on an organisation's ability to achieve its immediate objectives in uncertain and non-routine times.

Resilience in the context of critical infrastructure

The *Critical Infrastructure Resilience Strategy* notes “... some elements of critical infrastructure are not assets, but are in fact networks or supply chains”. In this context the strategy refers to resilience as:

- coordinated planning and relationship building across and between networks and sectors
- responsive, flexible and timely measures, and
- the development of an organisational culture that has the ability to provide an acceptable level of service during disruptions, emergencies and disasters, and return to full operations as quickly as resourcing allows.

As critical infrastructure organisations are essential to our economic prosperity and social wellbeing because of the functions and products they deliver during routine and non-routine situations – the resilience of critical infrastructure is of national importance.

Benefits of a resilience approach

Although the impetus for enhanced organisational resilience may require some increased investment in organisational capability (or at least a realignment of existing resources), general business benefits should be realised.

Valikangas (2010) emphasises that organisations with adaptive cultures, innovative thinkers and inner strength thrive in the face of unpredictable markets.

As such, building resilience has daily business benefits. These include:

leadership

- more successful outcomes from strategic and operational planning
- enhanced leadership capacity

organisational performance

- reduced disruption costs, including reduced insurance premiums reduced exposure to uninsured losses
- faster return to pre-disruption profits after disruption
- faster return to pre-disruption performance
- reduced need for regulation to meet community expectations
- enhanced reputation with stakeholders (e.g. community, regulators, clients)
- increased staff morale, commitment and productivity
- improved ability to attract quality staff
- generation of reputational and sustainable advantage
- increased market share

change ready

- increased foresight of emerging external threats
- enhanced ability to create innovative thinking, and
- improved ability to use adversity for change and improvement.

Resilience is not just sound risk management, effective emergency/crisis management or business continuity management. It is an organisational approach that embraces asset and resource protection, performance and strategic leadership, organisational development, and a responsive and adaptive culture.

It is about corporate governance, strategic people management and ensuring that an organisation can achieve its stated objectives for owners and stakeholders, even in the face of adversity.

In practical terms, the focus of resilience is generally on protection, performance and adaptation. These are discussed in the Australian case studies on organisational resilience, presented in the following paper.

It is recognised that the resilience maturity an organisation aims to achieve is a value judgement for boards or other governance bodies. An organisation needs to clearly acknowledge (to shareholders and stakeholders) that they have decided to approach adverse events and situations in a particular way. There are a range of such approaches, as outlined in the following table.

Decline	An organisation accepts that adversity may cause it to cease operating	<p><i>Ericsson and the Philips Albuquerque Fire</i></p> <p>When Philips had a fire in its New Mexico electronics production plant, their customer Ericsson did not spring into action the moment employees detected the disruption. Ericsson's employees lacked the urgency, mindfulness and passion to react quickly. Ericsson suffered production disruption and lost more than US\$400 million. Ericsson's competitors grew their market share.</p> <p>(Sheffi 2007)</p>
Survive	An organisation's resilience objective is to exist in a reduced form after adversity	<p><i>1997 Fire at Bankstown City Council Offices</i></p> <p>Bankstown City Council offices burnt down in July 1997. With good leadership and motivated staff, services were restored to the community quickly.</p> <p>(Fitzgibbon 1998)</p>
Bounce Back	An organisation's resilience objective is to regain pre-adversity position quickly and effectively	<p><i>2008 Hurricane Katrina and Mississippi Power's Response</i></p> <p>Following Hurricane Katrina, Mississippi Power grew from 1,200 staff to 10,000 in just a few days. A prior investment in developing mutual aid agreements with other energy infrastructure providers, extensive planning and training, strong supplier and regulatory relationships, exceptional leadership and empowered staff meant electricity supplies were restored to all customers in just 12 days. Mississippi Power received positive community recognition for its outstanding effort.</p> <p>(Sheffi 2007)</p>

Bounce Forward	<p>An organisation's resilience objective is to improve aspects of the organisation's functioning e.g. reputation, asset condition, future risk management, staff morale, market share etc so that in adversity it not only survives but possibly gains from the situation</p>	<p><i>Nokia and the Philips Albuquerque Fire</i></p> <p>By comparison with Ericsson, when Philips had the fire in its New Mexico electronics production plant, their customer Nokia quickly escalated the issue, conducting ongoing situational risk assessments. Through extraordinary efforts and intensive collaboration with its suppliers, Nokia effectively managed the event and significantly increased its share of the mobile phone market.</p> <p>(Sheffi 2007)</p> <p><i>Wal-Mart and Hurricane Katrina</i></p> <p>Wal-Mart was monitoring the formation of Hurricane Katrina prior to any public announcements by the US Weather Service. Staff were alerted and supply chains rearranged well before Hurricane Katrina reached the Mississippi Coast. Wal-Mart's response to restoration of customer services and support of impacted communities received national recognition. As a result of the success of the operation Wal-Mart's brand reputation was significantly enhanced.</p> <p>(Leonard 2005)</p>
-----------------------	--	--

An organisation's resilience objectives will reflect business direction, corporate culture, risk appetite and stakeholder expectations.

However, while organisational resilience objectives will be different for different organisations, with respect to critical infrastructure there is a government and community expectation that owners and operators of critical infrastructure will work to enhance resilience to ensure continuity of essential services in the face of all hazards.

Principles of organisational resilience in critical infrastructure

The following principles help to describe the concept of resilience:

- resilience is frequently defined as an ability to bounce back from adversity. While this is a useful definition in many cases, and is an often-desired outcome in a critical infrastructure context, it does have limitations. This is because organisations can use times of adversity to achieve positive change – so they should be open to both the possibility for bouncing back, but also taking opportunities to bounce forward
- resilience is dynamic and emerges from the complex interaction between a wide range of organisational attributes
- due to the diversity of critical infrastructure organisations, each may need a different mix of resilience attributes to achieve optimal resiliency. The appropriate mix of attributes is best determined by critical infrastructure owners and operators
- an all hazards, all threats approach to improving an organisation's resilience will better prepare it for unforeseen events, and
- achieving resilience in mature organisational systems can present challenges where organisations have experienced very stable environments and have developed systems and a culture aligned to that environment. In such instances, active strategies for resilience need to be deployed as a cultural change process to encourage the development and fostering of resilience attributes.

Resilience – behavioural attributes

The REAG has identified three broad *behavioural* attributes of resilience, which are detailed below:

Leadership and culture

The leadership and cultural attributes include:

- develops an organisational mindset/culture of enthusiasm for challenge, agility, flexibility, adaptive capacity, innovation and taking opportunity
- promotes a consistent and transparent organisational commitment to a resilience culture, values and vision, including a belief of ‘one in – all in’
- fosters an environment that supports agility, flexibility and initiative in decision making through trust, clear purpose and empowerment of employees
- encourages increased personal resilience by employees, and
- boards and senior executives engage and provide leadership appropriate to their position on organisational resilience.

Networks

The network attributes include:

- establishes relationships, mutual aid arrangements and regulatory partnerships
- understands an organisation’s community interconnectedness and its vulnerabilities across all aspects of supply chains and distribution networks, and
- promotes open communication and mitigation of internal and external silos.

Change ready

The change ready attributes include:

- promotes proactive anticipation and preparation for future challenges
- develops a forewarning of disruption threats and their effects through sourcing a diversity of views, increasing sensitivity and alertness, and understanding social vulnerability
- promotes empowered and broadly embraced organisational and individual self-efficacy, as well as enthusiasm for finding effective solutions to complex challenges
- promotes requisite decision making using both rational and intuitive abilities, and
- promotes critical reflective learning, lesson retention, knowledge sharing and continuous improvement.

These attributes can be applied to any aspect of organisational capability development, and if promoted and developed within an organisation – it will thrive.

For example, an organisation with a product development department exhibiting these attributes is more likely to have increased market share due to an inherent ability to identify opportunities and bring better targeted product to market more quickly than their competition.

The same applies in adversity. If the same organisation is presented with a critical set of circumstances it will have the ability 'to dig deep' and organise itself to manage through the situation and most likely gain advantage from it, whereas its competitors may not.

The Australian case studies in the following paper provide a number of insights to the businesses benefits of resilience.

Next steps

The REAG is supporting a range of initiatives to develop the concept and understanding of organisational resilience. This includes activities implemented under the Australian Government's *Critical Infrastructure Resilience Strategy*, such as:

- developing resilience champions to enable the development of resilience strategies and innovation
- education, including an introductory and advanced studies program in organisational resilience with the Australian Emergency Management Institute's knowledge-hub
- developing tools and resources, such as an organisational resilience body of knowledge, and a maturity model that will provide a framework to ensure the best resilience strategies emerge
- fostering cross-sectoral, national and global collaboration, including an organisational resilience knowledge network, and
- contributing to further discussion through publications, presentations and other forums where resilience is an existing or potential topic of consideration.

This paper will help to inform the above activities, and will provide a foundation to consider and assess future activities to advance the concept and practice of organisational resilience.

References

Australian Government's *Critical Infrastructure Resilience Strategy 2010*

HB 254-2005 Governance, *Risk Management and Control Assurance*

AS/NZS ISO 31000:2009. *Risk Management – Principles and Guidelines*

Fitzgibbon, M (1998) *Burnt But Back on Track*, National Emergency Response Journal 80 (6), pp 10-15

Gibson, C and Tarrant, M. E (2010) *A Conceptual Models Approach to Organisational Resilience*, Australian Journal of Emergency Management 25 (2)

Gittel, J. H, Cameron, K, Lim, S. G. P (2005) *Relationships, layoffs, and organizational resilience: Airline industry responses to September 11th* Michigan Ross School of Business, Positive Organizational Scholarship, Working Paper Series

Klein, G (1999) *Sources of Power: How People Make Decisions* Cambridge, MA: MIT Press

Leonard, D (2005) *The Only Lifeline was the Wal-Mart*, CNNMoney.com

Sheffi, Y (2007) *The Resilient Enterprise* Cambridge, MA: MIT Press

Valikangas, L (2010) *The Resilient Organization*, McGraw Hill

Acknowledgements

Marc Bellette	Australian Emergency Management Institute
Peter Brouggy	Banking & Finance Sector Group
Colin Chapman	Queensland Urban Utilities
Dianne Cooper	Australian Emergency Management Institute
Tim Cousins	Tim Cousins & Associates
Lawrence Cox	LIC Business Continuity Advisory Services
Helen Foster	Barwon Water
Dr Robert Kay	Incept Labs
David Parsons	Sydney Water
Dr Erica Seville	Resilient Organisations Research Programme, New Zealand
Robbie Sinclair	Intelligent Risks Pty Ltd
Paul Stoddart	Australian Government Attorney-General's Department
Michael Jerks	Australian Government Attorney-General's Department
Mike Tarrant	Australian Emergency Management Institute
Raelene Thompson	Australian Emergency Management Institute
John Valastro	QANTAS
Damian Fisher	Standards Australia
Peter Shepherd	Hatamoto
David Harris	Victorian Department of Primary Industries
Kellie Phillips	Telstra

Organisational resilience: Australian case studies

Contents

Resilience in business	20
A well played game has significant bottom line benefits.....	21
What about some Australian case studies?	22
Case 1: the lawyers and the accountants.....	23
Case 2: the hi-tech laboratory instrumentation company	25
Case 3: the wholesaler/retailer of household products.....	26
Case 4: the freight company.....	29
Case 5: the communications company.....	32
Case 6: the power station project.....	35
Case 7: the electronic design and manufacturing company.....	38
Checklist of lessons learnt.....	43

Resilience in business

The concept of 'resilience' as a formal business paradigm is still relatively young. However, as noted in the preceding position paper, there is a growing awareness of the need to develop the right behavioural attributes within an organisation that embrace and support the concept of resilience as a normal part of everyday business planning and practice.

Becoming more resilient involves the deliberate application of a range of tools, strategies and business paradigms that many Australian businesses will already be familiar with. How these come together is the key – and some of the many ways this happens, or doesn't, is illustrated in the following selection of seven case studies.

Generally the focus of resilience is often on: **protection, performance and adaptation.**

Protection is needed for business systems connected to highly distributed, unbounded network environments such as social networks, electronic networks or where critical assets and systems are exposed to the vagaries of the environment. These systems need to be robust enough to survive various assaults and/or intrusions.

Performance refers to the need to get things right the first time and to move quickly to correct errors. It has a task orientation with a specific focus – so it's important

to gain and retain first mover advantage, or improve business efficiency, whether as part of normal business or when recovering from a disruption.

Adaptation is required when circumstances change, demanding a change in the business focus, structure and processes. It is where experimentation, learning and divergent thinking are required to open up and explore new markets and ways of doing things.

While resilient organisations tend to have a strong commitment to protection, performance and adaptation, they also have flexibility to shift focus and alter the mix should the need arise, without compromising their core values.

A good analogy is preparing for a game of football.

What are the strengths required for the different positions on the field and what level of detail would you put in the game plan before the detail itself begins to restrict the players? Good preparation involves decent equipment, placing the players according to their strengths, developing a common understanding of the type of game they are to play but leaving the moment-by-moment decisions to the players themselves. In short, the aim is for the players to be aware of the state of play as it develops, communicate well, exercise good judgement and execute their decisions ably.

A well played game has significant bottom line benefits

A 2010 United States study of 520 large multinational companies was described in a white paper by FM Global entitled *The Risk/Earnings Ratio – New Perspectives for Achieving Bottom Line Stability*. It showed a clear positive correlation between the earnings stability of a company and investment in physical loss prevention.

Simply put, preventing the potential losses from fire and natural disasters, as well as investing in preventing human error and equipment breakdown, have confirmable bottom line benefits.

Some findings from the study ...

The risk of property loss is 20 times larger for companies with weak physical risk management practices than for those with strong physical risk management practices.

A location with weak physical risk management practices is more than twice as likely to experience property loss and consequential interruption to business.

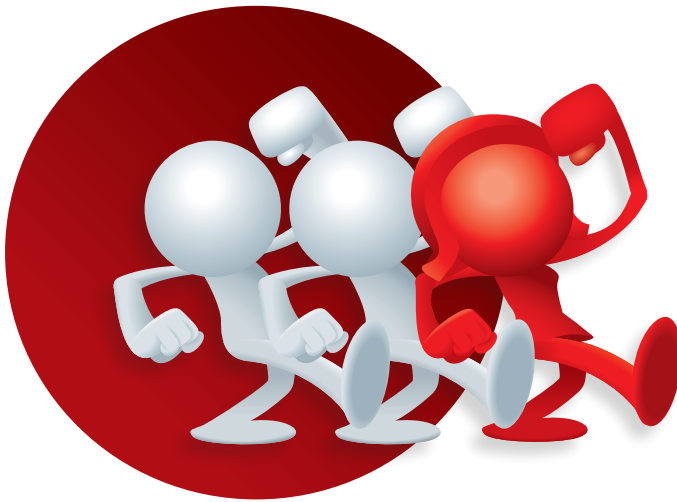
When the financial costs of these losses is factored in, the average loss per location with weak risk management practices exceeds US \$3 million compared with approximately US \$620,000 for strong practices.

The average risk of property loss caused by fire is 55 times greater for a company with weak risk management practices.

The severity of the fire loss exceeds an average of US \$3.2 million per loss for a company with weak risk management practices, compared with US \$725,000 for a company with strong risk management practices.

What about some Australian case studies?

The following seven case studies help illustrate some of the many different facets of resilience. They begin simply, and develop in complexity and detail, as do the issues they illustrate.



Case 1:

the lawyers and the accountants

A matched pair – different outcomes

This case compares the responses of two very similar organisations to a localised flooding from a burst water pipe. On the face of it the situation is fairly uncomplicated but the time to recover was quite different. In the first case the water hose leading to a dishwasher gave way, in the second it was an overflowing cistern in the office toilet.

Both organisations had about 35 staff in carpeted two storey office buildings, each about 450m². The first organisation was a firm of lawyers, the other a firm of accountants.

The legal firm – return to business as usual in six weeks

Two of the senior partners of the legal firm responded quickly and decisively to the discovery of the water but they did so independently. As a consequence, two plumbing firms, two electricians and two carpet restoration companies attended. While there was some initial embarrassment and difficulty allocating the work (none of the staff were informed or advised about the appointments) the matter was eventually sorted. Further complications arose due to lack of clarity, and sometimes contradictory instructions coming independently from each of the two senior partners.

They were urging rapid completion without coordinating or managing the work flow and many mistakes were made in the rush.

For example, when removing the carpet for drying, the contractors sliced through the computer network cables disabling the network. The difficulties continued with the temporary removal of half height office partitions and the relocation of staff while the drying process was underway. A dispute about the viability of drying versus replacing the carpet arose with the landlord, which further delayed resettlement. As a result, it took six weeks to repair and re-lay the carpets, return the office partitions and restore the network permanently.

During this time information from the senior partners about what was going to happen, what was happening and what was required from each of the staff was fragmented. Staff were unable to raise issues or point out problems as they arose. The senior partners were often too busy and many small problems were left unresolved. This led to a high level of frustration among staff along with a proliferation of critical comments. Divisions formed among the staff making matters worse. Most of the communication seemed to be focussed on why the process was not working and who was to blame rather than on the repair itself.

The accounting firm – return to business as usual in six days

One of the senior partners and the office manager teamed up together to discuss how they were going to respond to the incident. Whenever they discussed key matters staff were invited to, or they simply gravitated to, meetings held every few hours on the first day and early each morning and afternoon on subsequent days. The appointment and work orders for the attending contractors were clear and included an informal channel for the contractors to notify the team of presenting or latent problems. The information about what was going to happen and the potential impact flowed both ways and was conducted with an air of mutual respect. Levels of cooperation among the staff and with the attending contractors were high, with each going out of their way to assist the other. This significantly reduced the number and complexity of problems and normal business was resumed within six days.

LESSONS LEARNT

The culture of an organisation can have a profound impact on the duration of a disruption – particularly when it comes to how members share their understanding of what needs to happen and the impact this may have on all parties. In both instances, the organisations responded to the crisis in a manner that was an extension of normal problem solving and dispute resolution practices. Crises tend to reveal and magnify underlying strengths as well as weaknesses. If you think that your organisation's normal day to day problem solving ability could be improved, then it would be prudent to attend to that sooner rather than later.

“Crises tend to reveal and magnify underlying strengths as well as weaknesses”

Case 2: the hi-tech laboratory instrumentation company

No plan and underinsured – all they had was a common purpose and a will to survive

A company that designed, manufactured and distributed spectrophotometers and other hi-tech laboratory instrumentation was plunged into a dire financial position as a result of a fire and inadequate insurance coverage. The company was partially owned by an Australian bank in an unusual joint venture. The bank, as an active partner, wished to shut the business down and liquidate rather than attempt a recovery. Despite this the directors of the company united to engender a symbolic 'heroic' response among the staff, which coalesced after a few days into a common commitment of purpose and determination among staff. So much so that the company was able to negotiate extensions of time and finally demonstrate financial viability. Despite the objective financial assessment by the bank having written the company off after the fire, it is still operating and thriving today some 15 years later.

LESSONS LEARNT

The lack of an adequate insurance program, including the proper quantification of value at risk in relation to all insurable assets and consequential losses, can be an indicator of how an organisation approaches unforeseen risks. In this case, the company did not perform well, which added a considerable burden to the post disruption cash flow management. On the other hand, the company thrived on problem solving and the crisis magnified this strength with the emergence of an unusually strong sense of purpose and commitment among the staff. This kind of response must exist in some form beforehand as part of the company culture for it to emerge and be expressed in a crisis – and this can go a long way to offset lost or damaged resources. Resilience is multi-factorial and a determined, coordinated and cooperative approach can overcome many significant obstacles.

Case 3: the wholesaler/retailer of household products

No plan, poor leadership, culture of blame, heavy reliance on insurance for lost profits

A Melbourne based family business established in the 1950s as a wholesale business was the largest importer of Chinese household products into Melbourne in the early 1980s. At that time they were also a major supplier of such goods to the large retailers throughout Melbourne. The business also developed a retail arm which operated up to 19 outlets throughout Melbourne and regional Victoria under three separate entities.

The wholesale arm of the business was turning over \$14 million in the years leading up to an incident in March 2001. In that incident, a water main burst in the car park, flooding the entire office complex and wholesale display room.

As the water entered the building it ran over the main electrical supply to the building, including the supply to the computer system. As a consequence the main file server was compromised resulting in frequent system crashes, and corrupted product and customer databases. The company had been without local IT support for some time following a disagreement with their previous provider(s) and was left for some considerable time without a proper diagnosis or rectification of the problems. The company misunderstood the IT problems to be a result of the dust raised from the fans and de-humidification equipment used to dry the floors and walls. As a consequence, the corruptions in the data files continued to grow and interfere with business operations.



Staff productivity was also very low in the ten days following the flood. Staff complained about the noise, dust and smell but senior management was unable to implement any effective strategies to mitigate this. The drop in productivity in conjunction with the computer problems, as well as the noise, dust and smell had a major impact on trading. The flood had occurred just before Easter, which was significant, as the pre-Easter activities typically generated a high turnover of product with a high profit margin (including Easter eggs). This made up a significant portion of the annual income. When customers rang and could locate a staff member (the phone system was also experiencing problems) there was no reliable way of determining stock levels and many orders placed disappeared from the system as a result of data corruptions.

As a result, customers who were heavily reliant on the company became highly vocal and hostile, and a number ultimately litigated for the increased cost of finding short notice alternatives. Despite the demand for Easter eggs, the bulk of the stock could not be moved and had to be sold through the company's retail arms at heavily discounted prices. The net effect was a fall in gross profit from \$1.3 million in the preceding years, to \$392,202 in 2000–01 and to \$155,458 in 2001–02. The business has since been sold.

LESSONS LEARNT

This is an example of a profitable but non-resilient organisation where too much reliance was placed on the operation of their insurance policy for financial support. In this case the loss occurred at the worst possible time, when the level of liquid financial reserves was low due to the build up of stock in preparation for Easter. The company directors saw quite correctly that the level of disruption was disproportionately greater than the physical damage – but they had assumed that this would resolve itself in time. They were relying on the level of insurance being adequate with sufficient cover for any potential loss of profit, and that this would restore them financially in due course.

Insurance payments can only contribute to the recovery effort in a meaningful fashion if the insurance claim process itself is managed and supported adequately

Continued next page

In practice, the claims process often mirrors the company's response to the disruption as it is largely driven by the company being able to demonstrate the loss to insurers.

Calculating and proving the loss for a Business Interruption Claim can be as complicated as it can be confusing and it takes time to capture and present the necessary financial data. Unfortunately the lack of leadership and coherence within the company extended to the claims process itself.

The Loss of Profits insurance claim involved documenting and proving costs associated with:

- loss of profit margin on stock destroyed
- cost of dislocation of business activities
- non-fulfilment of standing orders
- breaking of contracts
- loss of customers to competitors
- continuing expenses: rent, payroll, interest, and

- ongoing inability of the business to attract customers.

The claim was only resolved some five years later, which was too late for the business. It did not recover and was ultimately sold.

Simply having adequate insurance is not sufficient. It needs to be integrated into a broader business/contingency management program that includes a flexible and adaptive management team with a strong working relationship with IT, telephony and other critical service providers.

*“Simply having
adequate insurance
is not sufficient”*

Case 4: the freight company

Clear decisions and a rapid response save the day. But should this have been necessary?

On a Friday afternoon in late 1998, the first of a series of computer screens linked into a freight company's national network displayed a warning that the computer had potentially been infected with a virus. The software had detected unusual activity through its heuristic analysis of programming commands and had flagged this as a potential threat. This was reported by staff to the IT department at head office for further instructions. Within half an hour three other sites reported similar problems. The organisation had a range of antiviral products installed with standards in place for ongoing updates or maintenance. It seemed that the virus was new. It was only being picked up by one particular antiviral software product and appeared to indicate that it was being transmitted via email. The IT department escalated the problem to senior management along with advice more or less along the following lines:

"In the last half an hour we have received reports of a viral infection in three regional offices. It seems that the virus is spreading through our network via our internal email and that it is highly likely that more of our regional offices as well as our customers will have been affected.

We do not have consistency across our network in terms of the antiviral software we use and many of our regional offices do not have the latest updates.

It is a new virus that is only being detected by one of the anti-virus software products and as yet we have no way of cleaning/removing it from our system."

After a brief consultation with the IT department the response from management was very clear and decisive. The network was shut down immediately to isolate the virus; the IT department was to form an antiviral task force assisted by competent computer users brought in from other departments. Their primary tasks were to complete an inventory of the system and the status of their installed antiviral software, as well as to work with a number of antiviral software providers on a solution.

The team immediately shut down the network and began ringing each of the regional offices to complete their inventory. It became apparent that the lack of IT skills in the regional offices was going to be a major problem and that much of the antiviral software was out of date. Concurrently, senior IT staff were in direct contact with a number of antiviral software houses, two of which were willing to work cooperatively on a solution. One was based in Melbourne, the other in the United States. At that stage neither company had a fix that could reliably identify and clean the infection. From

the freight company's point of view it was clear they needed a reliable fix that they could roll out across their network as soon as possible. This required approximately 2,400 new licenses. The Melbourne based company provided the first new software release but internal testing by IT staff revealed software conflicts while running Microsoft Exchange Server. This was the standard platform installed in many of the regional offices and considerable time was spent working closely with the Melbourne based group for a solution. Within ten hours the company based in the United States released a fix that did not appear to have the same level of conflict and the decision was made to roll out this product.



In addition, a small group of customer account managers was formed to liaise with the company's clients. There was some concern that by doing so, the company may be seen to be liable if a virus was found coming from their system. Despite this, management decided it was in their clients', and their own best interest, to provide reliable and useful information regarding the nature of the virus. They set about ringing and advising their priority clients that they had become aware of a new virus that was doing the rounds, that it was not yet being detected by the majority of antiviral products, and that they were working with a number of antiviral companies on a solution. As soon as they had a reliable fix they would be back in contact to let them know. This approach was received well by the clients and ultimately no claim for damages eventuated.

Installing the software fix across the network was a huge logistical problem due to the remoteness of some of the regional offices and the lack of local in-house IT skills. In addition, some of the existing antiviral software did not de-install correctly, which complicated the installation of the new software. To support the operation, 34 external contractors were engaged across Australia, many of whom had to fly or drive to the more remote regional offices to complete the installation.

The time from the discovery to the final clean and integration of the last regional office back onto the network was about 72 continuous hours. The program allowed for priority core services to resume late on the Sunday evening, with full completion the following night. The total direct cost of the exercise was just short of \$1.3 million.

“The response required clear, firm decision making, as well as the allocation of sufficient human and financial resources”

LESSONS LEARNT

A rapid and proactive response to problems in their infancy can prevent them from escalating to a major crisis. In this instance the rapid response resulted in minimal disruption to the company's core services. While there was some luck that it occurred late on a Friday, it had the potential to disrupt operations considerably if it was allowed to continue into the next business week. The response required clear, firm decision making, as well as the allocation of sufficient human and financial resources.

The second lesson to learn from this case is that a viral infection is a foreseeable event (and an exclusion on their insurance policy); and that a prudent and coherent antiviral program could have been implemented prior to the emergency for considerably less than the \$1.3 million cost of the emergency response.

Case 5:

the communications company

A draft business recovery plan and questions of contributory negligence

In January 1997, water contaminated with rust was accidentally discharged from a gas suppression system into a 350m² computer data centre (CDC). This affected \$120 million worth of computing equipment spread across 180 computer cabinets housing 70 different computer systems running approximately 83 different applications. The water had been left in the heat exchanger and some associated piping after a hydrostatic test that was undertaken during the commissioning process in 1994. This resulted in the formation of rust which was discharged into the room by the gaseous fire suppressant when the system was manually activated. The result was rusty water sprayed over and underneath all of the operating computer equipment in the CDC. The equipment was still operational but required decontamination. This created significant risks of malfunction and breakdown, which would have had serious consequences for the company. The recovery was ultimately successful, taking 18 months to complete and costing in the order of \$27 million. Despite this, the incident was not declared a disaster in terms of the Business Recovery Plan, and it was managed well enough so that it didn't cause any serious business disruption or revenue loss to the company.

The company brought proceedings against the relevant engineering firm and other defendants to cover the cost of the recovery effort. This also generated a multiplicity of cross-claims. At the time of the incident the company only had the one CDC and the Business Recovery Plan was in draft form only. A counter claim for contributory negligence was raised on the basis that a prudent business in the same position would have developed and implemented a disaster recovery plan and established adequate backup sites for any applications that ran on equipment in the CDC well before the incident in 1997, thereby minimising the cost of the recovery.

The business recovery plan

For many years the company had been working towards detailed recovery plans, the establishment of dual processing equipment for some computer applications, and the establishment of a disaster recovery site. The issue of data centres, the number of them, their size and location had been subject to frequent reviews since 1992, and in December 1995 a strategy of developing split data centres was established. This involved developing a purpose built second CDC (due for completion in May 1997, five months after the incident) while using a 'warm' contingency site as an interim solution.

In deciding on the business recovery strategies the company considered factors such as the amount of money that would need to be expended initially, the amount of money that would need to be expended in the event of a disaster, the availability of insurance, the availability of contingency plans, the testing of crisis management capability, and competency of management.



The counter claim for contributory negligence

The counter claim for contributory negligence was based on the argument that given the nature of the businesses and their reliance on computers and information technology, the company should, as a matter of normal business prudence and risk management, have conducted a business impact analysis in 1992. This should have occurred either before the first CDC was established or immediately after, and repeated annually as the business changed and developed. The company should then have reviewed the results of these analyses, developed a comprehensively documented business recovery strategy, and developed and implemented a disaster recovery plan in accordance with the strategy. That plan should have included the establishment of backup sites for critical equipment in the CDC, with adequate equipment installed to allow applications that ran on that equipment to be recovered within the timeframes identified in the business impact analyses. Finally, the plan should have been tested using walk-through exercises, simulations and live exercises, at least by 1994.

It was alleged that the company failed to exercise reasonable care, firstly, in not carrying out business impact analyses at a much earlier date and secondly,

having carried out the analyses, in failing to develop any adequate disaster recovery plans and failing to establish a backup site.

The criticism levelled in the counter claim was not that the company was indifferent to self protection, but that its efforts in that regard were inadequate. However, it was acknowledged that the establishment of a backup hot site would have involved expenditure of several million dollars with ongoing maintenance running into six figures per annum. It was the Judges' view that it would take a compelling set of circumstances to warrant a finding of contributory negligence in failing to undertake such expenditure.

In this case the company had taken reasonable care in developing strategies that considered factors such as:

- various contingency plans
- a risk management program
- completion of a formal business impact analysis
- backup data centre establishment costs
- disaster activation costs
- the competency of management
- the support of the major equipment vendors, and
- an insurance program.

LESSONS LEARNT

This case is a good example of how resilience does not need to have an 'all bells and whistles' protectionist approach. Instead it illustrates how many different complementary strategies can come together within an enabling management culture to support the organisation through a period of disruption or loss. The company is still operating very successfully today using a similar mix of strategies.

“The company is still operating very successfully today using a similar mix of strategies”

Case 6: the power station project

The escalating cost estimate of the damage

In June 1998 a fire occurred within the electrical services centre of a coal-fired power station, which was still under construction by a consortium of five international companies. It was due to come online in time to meet the peak demand in February 1999.

The fire burnt for eight hours before it was extinguished. The delay occurred largely as a result of the local fire brigade's lack of familiarity with the layout of the new building and the poor information regarding the source of the fire. As a result of the delay, fire combustion products, soot and later a cloud of steam from the fire fighting effort permeated the building into all the control equipment, cables joints, and field wiring marshalling racks. More critically, the cloud of steam condensed onto the surface of electronic assemblies and dissolved the water soluble fire combustion products forming a corrosive acidic solution.

The estimate of the cost of rectification rose rapidly from an initial \$5 million to \$90 million within the first few weeks. This change introduced a layer of complexity among the consortium partners, not to mention their insurers, which brought planning more or less to a halt six weeks after the fire.

One issue that spanned all consortium partners was damage (chemical, thermal and mechanical) to approximately \$23 million of electrical power and control cables. These cables fell into six major categories from field signal cables through 415 volt power cables to 11kV power cables and earth straps. The power company's Construction Superintendent issued a directive to the consortium that *work should not proceed on the restoration of cables until the coordination, processing, testing and acceptance criteria have been approved by the Superintendent*. This placed the recovery effort in a difficult position. No one member of the consortium was in a position to take a legitimate stand as each had only partial responsibility for the problem. With each of the consortium partners more or less keeping to their own territory, the issue was not going to be resolved internally.

An external group of specialists was formed to resolve the issue. It comprised materials scientists from two Australian universities, the research and development arm of the power cable manufacturers, a specialist electrical power engineer from the United States, and a disaster recovery specialist. The output from this group was a set of reasoned and practical procedures based on the overlap between the various expert opinions, which came under intense scrutiny but were ultimately accepted, enabling the recovery work

on the cables to proceed. The plant came online in time at a total cost of \$50 million to meet the February peak demand, thereby avoiding significant (uninsured) liquidated damages claims.



LESSONS LEARNT

Understanding the nature and extent of the damage is fundamental to organising an effective response. It is the one area where there is often significant disagreement between the various stakeholders – and it is often assumed by business continuity planners that it can be determined in a timely fashion. The difficulties, and therefore length of time, in reaching agreement between the various stakeholders is not something that is often considered, yet it is often precisely a clear understanding of the nature and extent of the loss that drives the recovery process. This is particularly true for manufacturing plants where a backup of the process is often not possible.

In this case, the roles of the various consortium partners in the construction of the power station were clearly determined by formal contract. This usually worked well for the majority of site complications or construction problems encountered.

Any problems that fell outside this arrangement were dealt with quite adequately in the regular weekly site meetings. In some ways, this tight coupling served the construction project well. However, the scale and complexity of the disruption brought about by the fire exceeded the ability of the consortium as a group to make a competent determination of the nature and extent of the damage – with expected costs ranging from \$5 million to \$90 million. Getting a firm grip on this was fundamental to progressing the recovery effort.

If a determination of the nature and extent of damage is inadequately backed up with objective evidence then the credibility of the determination and therefore stakeholder buy in is difficult to obtain. Overstating the extent of damage places an unnecessary burden on the post-disruption capital investment strategies and cash flow, whereas, understating it delays a timely and effective resolution, again impacting on cash flow.

It is clearly beneficial to pre-arrange roles and responsibilities prior to a crisis in order to improve cooperation and coordination during a crisis. Beyond that, however, much rests on having an accurate determination of the nature and extent of damage. In some instances this will involve third parties with whom the organisation has had no previous or meaningful contact. Resilient organisations are able to include them quickly and form a productive working group to make a determination that is accurate, backed up with objective evidence that will assist buy in from concerned stakeholders.

Case 7: the electronic design and manufacturing company

Bouncing back while adhering to core values

This company can generally be classified as a hi-tech business that specialises in the research and development, production and distribution of safety and test equipment for telephone lines and pipe works. It is a major contributor to the operations of critical infrastructure facilities and services in Australia.

In June 2001 a fire severely damaged the entire production facilities, 80 per cent of stock on hand, and some 40,000 products. This occurred less than three months after the business and production facilities had moved to new premises.

The major issues that confronted the business after the fire can be summarised under the following eight subheadings:

- i) **working capital:** the company had more than \$1 million in cash reserve before the fire but the subsequent delay in the recovery of insurance money and the loss of sales meant deterioration in all aspects of the working capital
- ii) **trading stock:** prior to the fire, the company had six major product lines. This included a product developed over the previous 24 months that was introduced in September 2000 to fill a niche market.
- iii) **plant, machinery and test equipment:** the fire destroyed most of the plant, machinery and test equipment built over 30 years, including some special equipment that was not readily available on the market
- iv) **tools and jigs:** the fire destroyed 43 out of 46 specific tools and jigs. This made manufacturing of products very difficult and in some cases forced the company to abandon or replace a couple of product lines permanently



- v) **intellectual property:** the damage to the company included technical drawings, engineering notes, prototypes, production models, test jigs and the ISO 9000 QA documentation and samples. Rebuilding from this loss proved to be the limiting factor in the speed of the recovery
- vi) **customers and suppliers:** the crisis mainly affected customers and one major customer that lost confidence in the ability of the company to survive the crisis, shifted its orders overseas, and refused to award further contracts on offer before the fire
- vii) **insurance:** the company had adequate cover in place, however, the insurance response struggled for eight years due to the technical complexities of quantifying the claim
- viii) **staff:** there were staff resignations from senior positions in the six to eight weeks following the fire and high levels of uncertainty and ambiguity surrounding the company's future.

The company should not have survived, but it did and now has operations in Vietnam and the United Kingdom.

The issues that confronted the company can be analysed in terms of impact on: organisational strategies, organisational structures, organisational culture, and the individual personalities and character of the people involved.

Impact on organisational strategies

The company developed four major parallel strategies.

The first was to supply existing contracts as best as possible on the major product lines. The products that were considered to have the greatest positive impact on sales were considered first in the context of availability of raw material and undamaged/repairable production equipment. Customers with existing contracts were given priority rather than selling to new customers or new markets.

The second strategy was to restore the fire damaged building and move the production process from the temporary location, which had very limited space.

The third was to preserve what remained of the quality systems and protect the ISO 9000 accreditation from loss or suspension – this was vital for the company's customers and to reconstruct the lost intellectual property.

The fourth strategy was to rethink the design of the tools, jigs and electronic test equipment so the future productivity of the business would be improved.

The contribution of the above strategies is calculated to be an increase of \$380,000 in terms of the net present value of the company over the five years that the disruption continued to affect business operations. Without such an effort it is unlikely the company would have survived.

Impact on organisational structures

The impact on the organisational structure can be thought of in three phases: before the fire, in the weeks immediately following the fire, and after the personnel changes in senior management.

Before the fire the organisation had a hierarchical structure with all key decisions, in all areas of business, being referred to the general manager. In addition, the engineering department was reported to have been fairly conservative, governed largely by the dominance of a few senior knowledge holders where there was a focus on incremental development in an established engineering context (and market).

The weeks immediately following the fire were characterised by confusion in the power balance within the company. The loss of technical drawings, engineering notes and prototypes was a de-stabilising factor as the senior engineers were faced with having to solve problems without the specific detail that would

normally be available. Their role, immediately post fire, had also been subverted to the pressing financial and operational needs of the company.

After the personnel changes in senior management the organisational structure changed to be flatter and decentralised, where responsibilities for key operational decisions were made within each department. The strategic goals for the company, however, remained firmly the sole domain of the general manager and operational matters, including financial management were managed by a three person management team. The core engineering team operated independently in all but the most pressing operational imperatives.



Impact on organisational culture

The company had already embarked on a road to diversify their product range and expand their market. However, the drive for this initiative required both the finance department and the engineering department to shift from incremental improvement in a narrow market, to active innovation and financial management in a broader, much riskier market. This required a fundamental change in thinking across the organisation to follow the new leadership, and in the two years leading up to the re-location this was beginning to change.

The resignation of some staff provided an opportunity for the general manager to recruit a new leadership team with a better fit in terms of their decision making style. The new staff included the former operations manager who had started his own business and the external accountant who was already familiar with the business. The new atmosphere changed from a sense of working in conservative silos 'grinding out' a stable product in a mature market, to one where cooperation and mutual respect flourished with the possibility of developing new innovative products.

Impact on personality and character of individuals

The occurrence of the fire suddenly meant each of the senior decision makers had to accept considerably more responsibility and accountability for the survival and future wellbeing of not only the company but their personal futures as well. There were certainly no guarantees that the company would survive. Previously they had relied on the company for direction, stability and personal confirmation, but after the fire they had no clear direction, the situation was unstable and they were expected to perform well outside their comfort zone. This reached a crisis point at the six week mark and as a result, senior decision makers resigned, allowing a new decision making team to form.

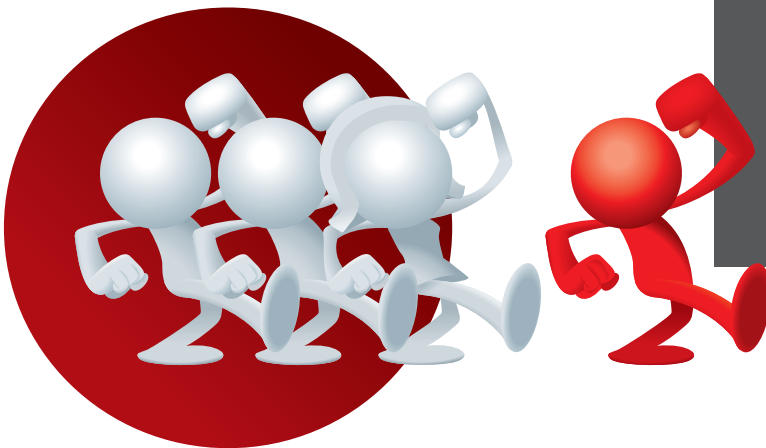
The new team consisted of the general manager, the former operations manager and the external accountant. Among them was an atmosphere of quiet confidence, which seemed to extend to the larger workforce as a sense of personal worth and security within the company. As a result, general morale appeared to improve quite dramatically.

LESSONS LEARNT

There are two surprising outcomes from this study. The first is that 'bouncing back' after a disruption needs to be tempered with the idea that the bounce back should not proceed any faster than adherence to the organisation's core values would allow. In this case the company's long term commitment to quality with an emphasis on the value of the product, not price, held even under extreme duress.

The rate of the recovery was then largely determined by the speed at which they could restore their intellectual property and rebuild the test equipment and tools, which was the cornerstone of their quality program. To rush this might have meant an improved cash flow but with it, an increased risk of the product failing out in the field, with implications for reputation, future tenders and viability of new product development.

The second outcome was the ability to use the opportunity offered by the staff resignations to quickly re-structure and build a new management team that could move the organisation rapidly to a more flexible and adaptive way of operating (to some extent, 'bounce forward'). This not only provided what was absolutely essential to protect the company's cash flow, but allowed for the real possibility of developing new innovative products.



Checklist of lessons learnt

These case studies help demonstrate some of the attributes needed to achieve resilience, providing real life examples of protection, performance and adaptation.

The following checklist provides a rundown of the lessons learnt from these case studies. While not exhaustive, this list includes some of the behavioural attributes associated with resilience discussed in the preceding position paper. As such, it will help to guide organisations interested in pursuing a resilience approach.

Does your business have:

- ☒ strong leadership with clear, firm decision making?

- ☒ a management team that works well together, is flexible and adaptive?

- ☒ clear channels of communication?

- ☒ good problem solving ability?

- ☒ a culture of cooperation and mutual respect among all staff?

- ☒ clear and strong core values?

- ☒ adequate insurance integrated in a broader business/contingency management program?



