



## The Learning of Lessons

Terrible bushfires have ravaged my home state this past fortnight, and many Victorians have suffered devastating loss.

Thank you to those many readers of The Infonomics Letter who have taken time to contact me and check on our welfare. Although my partner's home is in a high risk area, we were fortunate to suffer no direct loss on this occasion.

Some of our friends have been less fortunate. At this stage I know of three close friends who live on small farms in the burnt regions – one has lost everything, another lost all the buildings, and another lost outbuildings, machinery and fences.

It's not the purpose of The Infonomics Letter to explore the bushfire and community phenomena at length. Notwithstanding, there are some elements of the reality we as a nation have just experienced from which we may draw broader learning. Already, a Royal Commission (the most intensive form of investigation provided by law in Australia) has been established, and it will seek to identify the lessons we need to observe, for our future safety and wellbeing, and that of generations to come.

Another extraordinary event occurred recently in New York, when an Airbus A320 operating US Airways Flight 1549 suffered a major bird strike, knocking out both engines. For extensive coverage of this event, one need only browse the internet – there are dozens, if not hundreds, of pages dedicated to the event and the captain who succeeded in ditching the plane into the Hudson River with no loss of life.

Aviation is another field in which there is intensive scrutiny of everything that goes wrong, so that lessons are learned, and precautions are taken to limit the chance of, and minimise the consequences of future failures.

The Learning of Lessons thus is an appropriate and timely theme for The Infonomics Letter of February 2009. As always, I do hope that you find it useful, challenging, and entertaining.

This issue of The Infonomics Letter is dedicated to the memory of those many unfortunate people who died on Black Saturday, February 7, 2009. May they rest in peace.

Any readers wishing to assist Australia's bushfire victims may donate online to the Australian Red Cross at [www.redcross.org.au](http://www.redcross.org.au).

Mark Toomey  
18 February 2009.

## Preventative Medicine

The fact that Captain "Sully" Sullenberger was able to put his crippled plane down on the Hudson River is a testament to the value of training, experience and rigour. Given that this was his first, and hopefully last, experience of doing such a thing, one might wonder how he was able to do so with precision and aplomb. Actually, there was little luck or guesswork involved. The good Captain would have completed similar manoeuvres many times in the simulators, probably for several different aircraft types. Such training sessions, backed by classroom discussions on theories and alternatives, plus the in-depth knowledge of their aircraft that is a core requirement of airline pilots, would have given him hands-on experience of applying some profoundly simple, yet incredibly demanding rules for landing (airspeed correct, nose up, wings level) under extreme duress, so that his brain could be focused on dealing with the major problems, rather than the core routines that he would have done automatically.

Training, core knowledge and practice are essential parts of an aviator's life – and especially so for those who are airline pilots.

In an interview recently, Sullenberger said: "One way of looking at this might be that, for 42 years, I've been making small regular deposits in this bank of experience: education and training, and on January 15, the balance was sufficient so that I could make a very large withdrawal."

He makes a profound point – that we need to keep practicing if we are to lock-in and retain skills that we may need at short notice. Just going through a routine once, months or years ago, probably would not result in the capability one needs to deal with a problem when it arises. If one truly wants to be able to handle a problem competently, one must frequently and comprehensively practice dealing with problems – and because problems have an inconvenient habit of arising without warning, and without following any rules, the practice must be organised such that one learns how to deal with both probable and improbable situations.

How much effort do we put into preparing for even the probable problems, when it comes to information technology use? Is it sufficient? The operators of a Melbourne data centre servicing several major Internet Service Providers may well be asking those questions at present. During the heatwave that preceded the bushfires, the demand for electricity exceeded the capacity of the grid, and load-shedding pushed that data centre onto standby power. But something went wrong, and the standby

diesel generator did not spring to life. In a short while, the intermediate backup batteries failed, and the centre was shut down.

No doubt an investigation will identify the cause of the failure – but will this investigation be thorough? How far will it drill down? Will the conclusion be merely that “the diesel generator failed”, or will it identify why the diesel failed, why the failure could not be promptly resolved, and what should be done in the future to ensure that no such situation occurs again?

While there are many questions that could, and should be asked in hindsight, there are also several that might have been asked to test readiness for dealing with such failures. These questions go beyond the bland “Have you conducted a disaster recovery test” that seems to be a staple of many audit checklists:

- What proof exists that normal operations can be maintained in the event of a failure in the main power grid?
- To what extent can normal operations be maintained in the event of a protracted failure of the main power grid?
- What arrangements are in place to ensure proper and sustained functioning of emergency power supplies?
- What assurance is there of timely intervention by properly skilled and experienced personnel in the event of problems with emergency power supplies?

As we discussed in last month’s Infonomics Letter, there has been an apparent trend for organisations to cut costs by reducing the number of people involved in middle management and support roles. How many organisations, as a result of these decisions, no longer have the capacity to properly maintain, test and practice their emergency procedures? How many of them have emergency generator systems that have not been tested – perhaps not even started up – for months and years? How many of them have an emergency diesel generator, but are blissfully unaware that diesel fuel has a short shelf-life and must be refreshed at regular intervals, if it is not used? How many organisations would find, if the above questions were answered through a rigorous, independent review, that their power-failure precautions are inadequate in the context of their current and ongoing business?

In Australia, and perhaps in many other parts of the world, the constantly growing demand for electricity, combined with the ever-increasing demand for information and connectivity from an impatient population means that it may no longer be sufficient

for many businesses to rely on the main power grid. The overriding question, to which all of the above are subsidiary, is: “How long can our business survive in the event of a major and protracted disruption to mains power”.

Just how far we delve into these questions clearly depends on the nature of the business we are operating, and the demands and expectations of our customers. To properly answer the questions demands a very clear understanding of the business. For example, in the case of the internet service providers which went off the air because of the power failure, what sort of customers do they have, at that time, and what use were those customers making of the system. If we took a naïve and simplistic view, we might think that on a Sunday afternoon, the major workload would have been social networking and file sharing. But if we thought about the fact that the same day was one of extreme bushfire risk, we might also have seen that a significant part of the workload might have been individuals keeping well aware of the fire situation – the internet having become a pervasive and often first-choice source of information.

While this discussion is focused on one type of problem – the possibility and consequences of mains power failure – it is important to recognise that at an operational level, many different problems can arise, and disrupt the systems on which business depends.

Thus, the questions that organisations need to ask themselves start to become a little more fundamental:

- To what extent do the various aspects of business operations really depend on information technology?
- What are the possible failure modes that could cause disruption to our business, and how do we protect against them, and how do we recover of the protective measures fail?
- How do we prepare for, and protect our business in the case of less likely, or previously unidentified, failure modes?

If US Airways, and Captain Sullenberger had not asked these questions, known the answers, and practiced to develop and hone their skills, chances are that flight 1549 would have been another event where all aboard perished.

Does your organisation take effective precautions against expected and unexpected problems?

## Human Nature

In Australia’s bushfire prone areas, residents are urged to have fire plans, and to activate their fire

plans at times of high risk. Two strategies are promoted: leave early; or prepare and defend.

The "leave early" strategy is for those whose homes are considered indefensible. The "prepare and defend" strategy is for those who have taken precautions to minimise the opportunity for fire to attack, and to resist an attack in the event that the precautions are insufficient.

While these strategies have very strong contrast, each can work, when measured against the goal of saving human life. One sacrifices property to minimise the risk to people – the other involves a calculated risk, and demands a fallback plan. But there are already indications that the strategies were ineffective in the maelstrom that Victoria experienced on February 7, 2009.

My partner and I had direct experience of one of the problems: our teenage family members were reluctant to leave their home early on the morning of the fires. They argued that the adults were being needlessly cautious – that there would be plenty of time to leave if a fire came our way. How wrong they were! Eyewitness accounts from credible people say that in some areas the flame front was moving at between 120 and 200km per hour – between 80 and 120 miles per hour. Our reality was that from first sight of flames, we would have had less than a minute to evacuate the house and get into the car, and then we would have had to drive at suicidal speeds to stay in front of the flames. Of course, such a scenario is impossible – which is why our fire plan rigorously follows the advice of experts – leave early, before there is a significant danger, and stay away until after the danger subsides.

A key part of the problem here was that the advice relies on people all having a clear and shared understanding of the risk. But the teenagers had no prior experience on which to frame the advice of the experts. When the last massively destructive fires attacked Victoria in 1983, these children were simply not here. In fact, no person under 26 was here, and considering the age people need to be before they can take on board such dramatic lessons, it would be fair to say that few, if any members of the general public under the age of 35 would have any real understanding of what a serious bushfire can do. Thus, many people, including our teenagers, would have had a flawed understanding not only of the risk, but also of their ability to deal with the inferno when it came.

It seems clear in hindsight, that education about the risks and dangers, and the need for thorough preparation, planning, and practice, are essential parts of being truly prepared for, and surviving bushfire. In the many stories of tragedy and triumph arising from the fires we have just seen,

there will be clear examples of those who simply had no understanding of what might happen, and of others who had a very clear understanding.

We see another perspective on human nature in a report about Cactus Flight 1549, which describes how the outstanding effort of Capt. Sullenberger was nearly brought undone by one panic-stricken passenger. Rather than staying seated in the brace position, this passenger apparently leapt to a rear escape door as the plane touched down – opening it and causing the icy river water to flood into the back section of the aircraft. There was a danger that the plane could have been filled with water and sunk within minutes. Luck was on the side of the passengers and crew.

Victoria's bushfires and the Cactus 1549 incident provide a lens through which we can focus on the very core of Human Nature – the diverse ways that human beings behave. Some are thorough, others less so. Some believe what they are told; others need to experience the lessons directly. Some believe deeply in their own capacity to overcome adversity; others have little faith in themselves. Some believe that fate will never befall them; others believe that dealing with problems and disasters is "someone else's" job. Some can follow instructions and work to a plan under pressure; others panic, or become confused. These incidents also open a window of understanding to the differences in behaviour of people who are well prepared with sound knowledge and skills, compared to those who are uninformed and unprepared.

Is there any difference between the behaviours we are discussing here, and what we see in the world at large, in the context of information technology use? We are regularly reminded that information technology, while essential, is also risky. Some organisations take these warnings very seriously, yet others are reluctant to take precautions. Some organisations invest in precautionary measures to head off problems, and to deal with those that cannot be headed off; others wait til problems arise before reacting, and in doing so often find themselves poorly equipped to handle them.

Understanding human nature and the way people respond under stress is vital to bushfire survival. Does the same hold true when problems occur with IT? How would your organisation behave?

## **Securing investment funding**

A recent article in an Australian IT industry magazine (MIS) reported on the industry concerns about the fact that their customers are cancelling, postponing and slowing the pace of major IT initiatives, because banks are reluctant to provide investment funding to those organisations.

The industry acknowledges that in the current economic climate, risk is a paramount concern for the bankers, but nonetheless urges a more even balance between risk and what it calls "business essentials".

But how much risk should the banks take? When it comes to information technology, there is an extensive body of research, old and new, that confirms the high levels of risk still prevalent in IT investments. Indeed, research soon to be published by a friend of Infonomics reveals that 70% of projects in a global survey did not meet the objectives for which they were launched.

However, there are self-evident and well-proven ways to increase the chances of success for any IT investment. According to leading academics, including Peter Weill and Jeanne Ross, an effective system of governance for information technology corresponds directly to improved corporate performance and value. In the same vein, KPMG reported on the results of a global survey of their customers, saying that an effective governance regime is a vital part of increasing project success rates.

It follows that organisations able to demonstrate an effective system for governance of their IT use should be regarded as a less risky investment for bankers. The availability and price of borrowed funds might be linked to measured performance against a robust standard for governance of IT.

ISO 38500 is a robust standard for governance of IT, and Infonomics' experience of assessing organisations against the standard is that most organisations are seriously deficient in key areas. But the assessments that we have done also show opportunities for straight-forward improvement, with significant benefits in reduced risk, more tangible value from investments, and better targeting of investment resources.

Therefore, one way in which IT organisations might increase demand for their services is to work with their customers to improve the customers' governance of IT, leading to an improved risk profile and, perhaps, a better chance of obtaining funding for new investments.

Working with the banks to establish guidelines might make such a scheme very attractive.

## Feedback

It's wonderful to receive positive reinforcement, and this month I thought I should share some of the comments that readers have made:

- Great read. The reality is that the IT profession seems to struggle with presenting Board level proposals arguing for the capital required for IT investments.

However I have a very narrow sample and can not be sure this is universally true. If a Board of Directors does not understand the value delivered by IT, then it is hardly surprising the company will be in distress if the IT resources are cut too deeply during an economic down turn.

For the value of IT investments, I am firmly of the opinion that Boards of Directors hardly know why they have to spend heavily on IT most of the time. This is largely due to the very high costs of legacy system maintenance, rather than projects to improve performance.

Seems to me there is many areas of IT in business and government that need to be improved.

*Robert. The Institutional Corporate Governance Network.*

- I liked "Is Value Required". The short answer, of course is: YES! As you suggest. And the change of focus to benefits hits the nail on the head. This was one issue that tested us while developing the Business Case process for (major infrastructure company). I suspect your words would have make our work a little easier! Simply because they paint a clear picture. The notion of benefits, how to define and quantify them, then measure them, for some becomes just too hard! There's almost a fall back to a - 'them magic will happen', moment. Which we know is a triumph of hope over experience!

All this relates to small business. The process and rigor hold, it's making sure that the reduced quantum don't seduce folk to not follow through. "It only matters for the big guys!"

*Bob.*

## Governance of IT Conference



BSI British Standards has announced a conference on governance of IT, to be held in London on May 20 and 21. Infonomics is delighted to be supporting the conference, at which Mark Toomey will be speaking on the case for adoption of ISO/IEC 38500.

See [www.bsigroup.com/it-governance](http://www.bsigroup.com/it-governance) for details.

## Corporate Governance of IT Education

Infonomics is working with the Australian Computer Society to deliver briefings and masterclasses throughout Australia during 2009, as part of the ACS Education Across the Nation (EdXN) program. For full details, see [www.acs.org.au](http://www.acs.org.au) and search "Find an Event" for "ICT Governance".

We are also developing plans for masterclasses in the United Kingdom and in Germany, during May. For details, please refer to the Events page on [www.infonomics.com.au](http://www.infonomics.com.au).