



## Staying Alive, Getting Smart

Welcome to the final Infonomics Letter for 2010. Yes, this is the catch-up, where publication reverts to the early part of the month, beginning in January 2011.

An April 11, 2008 announcement by British Airways chief, Willie Walsh perhaps highlighted an uncomfortable new role for Chief Executive Officers – that of apologising for business service failures that have been substantially due to problems with IT.

Perhaps it's time to set up a "hall of fame" for CEOs who have had to endure this painful experience. As regular readers of The Infonomics Letter are well aware, Virgin Blue chief John Borghetti would be one of the more recent members.

But already the 24 hours of disruption to Virgin Blue's customers has been transcended, at least in volume of press and public commentary, by a breakdown in the overnight transaction processing at National Australia Bank – one of Australia's four majors. On November 29, NAB's CEO, Cameron Clyne secured his lifetime pass into the gallery by way of full page apologies published in daily newspapers.

As I said last month, there is rarely any shortage of case examples to provide the grist for this journal and the temptation to explore the possible lessons from NAB's experience is too great – so we lead with a discussion in **"Red-faced Bank"**.

NAB's experience highlights the importance of proper response to failure. To illustrate how this might work, **"Learning Lessons – the Qantas File"** takes a brief look at a recent aviation incident – the engine explosion in a Qantas A380 – and proposes parallel questions to be asked about IT failures.

Long-time friends of The Infonomics Letter will recall my [enthusiastic response](#) to the landmark report into the Australian Government's use of IT, delivered by British expert Sir Peter Gershon. Those who saw my comments in [August 2010](#) however will know that I have not been impressed with the implementation of Gershon's recommendations. Now another independent expert, Dr Ian Reinecke has delivered his formal report on how the Gershon recommendations have been addressed. **"Reinecke echoes Gershon"** explains why the new report hasn't made me feel any better, other than by confirming that there is still significant opportunity in front of us.

We've completed a summary of the October 22<sup>nd</sup> Monash/Deakin **"Seminar on Governance"** of IT.

My home state of Victoria has a new government, and a **"New Opportunity to Improve"** its own governance of IT. It needs to do so promptly!

Mark Toomey  
2 December 2010

## Red-faced Bank

The message to customers from British Airways' chief executive Willie Walsh was succinct: "Since Thursday 27 March (2008), when Terminal 5 opened, we accept that the service we have provided our customers has not been good enough. We are extremely sorry for this".

Equally succinct was the message from NAB chief executive Cameron Clyne in his nationwide apology to customers published on 29 November 2010. Clyne appropriately acknowledged the potentially significant impact of a problem with processing transactions on the night of November 24<sup>th</sup>. He acknowledged his customers and staff, and gave assurances that all financial losses incurred because of the problem would be made good. Finally, he confirmed that the fault has been resolved, though some correction to accounts was still required.

NAB's problem came at a time when Australia's major banks have been the target of considerable market resentment as they post substantial profits while simultaneously elevating interest rates. The press was ready to tear to pieces any bank that gave its customers grief and by the time the problem was 24 hours old, the bank was not only dealing with an IT problem – it was also in the midst of a public relations crisis of significant proportions.

Not only did newspapers around the nation post story after story on the problem, they also opened their comment channels to let the public vent. Discussion ranged widely from bland individual status reports from individuals who did or did not have any money, to speculation on the likely causes, the perceived arrogance of the banks in general, the performance (good and bad) of the bank staff and so on. More than a few pointed to the issue of modern society's dependence on reliable IT. [One comment](#), posted by "jim" at 3:37 PM November 26, 2010 says: *"hahaha one IT mistake, tens hundreds of thousands impacted (virgin blue, queensland health payroll, nab, etc etc)... company dumbos had better wake up to how important IT is and start treating it with respect"*.

Indeed, Jim has a point, however irreverently he makes it. In modern society, we have become conditioned to IT that mostly works and when it goes wrong, it can have a seriously debilitating effect that takes hold very quickly.

On the surface, banking for most people is a very simple business: put money in; take money out; pay bills; borrow and pay back; and so on. But underneath the covers, banking is an extraordinarily complex business that even with today's advanced technologies still requires unimaginably vast volumes of computer software to deal with every nuance of

banking products and their associated legislative obligations – let alone the programs needed to just run the business. This complexity alone poses significant risk – but for NAB and many other banks, the complexity of the software required is greatly exacerbated by age. Many of the banking systems of today are between 20 and 40 years old. They were designed in days when computing equipment was orders of magnitude more expensive than it is today, and when the boundaries of capability were much tighter. Banking systems from the 1960's, 1970's and 1980's had to be designed to spread the workload so that an 8 hour business day could, for very straight forward logistical and economic reasons, be spread out over 24 hours.

The design of banking systems in that era included a great deal of attention to controls – but it wasn't fool proof. From time to time events could occur that resulted in a problem that could interrupt processing. Bad transactions were almost routine and continuity of the business depended not just on controls to detect them, but highly skilled operational personnel who knew exactly how the systems worked and what to do to ensure that individual incidents did not present an impassable barrier to keeping the majority of account records up to date. Further controls provided strong audit trails of every action taken to resolve a problem transaction and ensure that it was correctly processed as soon as possible.

During the time when many of the still-current banking systems were being built, most of us lived in the world of cash and cheques. We would visit the bank once a week to deposit our pay, spreading it across our cheque, savings and loan accounts. Then along came credit cards which, like cheques, involved a paper transaction record that would become part of that 24 hour extended banking day, processed not individually, but overnight along with thousands of like transactions. Gradually we advanced to using an ATM for some transactions and then, a little more than twenty five years ago, we extended our demand for banking services with the now ubiquitous eftpos machine. In the late 80's and early 90's, telephone banking gave bank customers a much longer day in which they could transact, and the increasingly stressed accounting systems, still basically oriented to an 8 hour day, had to cope with an extended and ever more diverse workload. As the century drew to a close and a new one dawned, we extended our demand further to include internet access to banking from anywhere in the world, thus hammering the final nails into the death notices for banking systems everywhere. Systems designed for an eight hour banking day in an era of extremely expensive technology cannot be expected to cope with the rigours of our 24 hour society, even when the cost of IT equipment is relatively far lower.

Put simply, as the business of banking has changed beyond recognition during the past 30 years, many banking systems have not kept up with the pace of change and now, as so comprehensively demonstrated by NAB in the past few days, the limitations of those systems are becoming a significant business issue.

The comment referenced earlier, from "Jim", is therefore quite apposite. Nowadays, when IT is not fit for purpose, and fails to do its job properly, the consequence is not merely a delay in some back office functions. Rather, IT failures today often have a significant debilitating impact on the business and its stakeholders. Among other things, treating IT with respect includes understanding its limitations and guarding against the consequences of failure. It also means maintaining investment to keep systems in good order, and replacing them when they no longer suit the evolving business model. Further, it means maintaining a level of expertise at close call so that when a problem does occur, it can be assessed, isolated and resolved without impeding other business activity.

As always, NAB's experience can be constructively discussed in the context of the six principles for good governance of IT set out in ISO 38500. The principles also provide the backdrop for questions for CEOs and directors to ask about their organisation's dependence on IT:

**Responsibility:** While most large organisations have a CIO and formal arrangements for supply of IT services, the consequences of an IT failure are now, unequivocally, business consequences. Therefore it is essential that business leaders and managers are responsible for ensuring that there is sufficient investment to keep the primary IT business systems in good working order aligned to the contemporary business, and that there are suitable arrangements in place for promptly resolving any problems that may arise. *Who should make the key decisions about investment in generational change in your organisation's IT? Do those responsible step up to the challenge?*

**Strategy:** IT that underpins the business should be aligned to the needs of the business, just as the business should take appropriate advantage of new IT that enables the business to deliver new products, services, channels and relationships. There should be ongoing attention to ensuring that IT evolves to suit the current business and enable its future growth. *Are your organisation's IT systems well suited to your current and future business model, or do they pose constraint and risk that may be, especially in the eyes of your customers, unacceptable?*

**Acquisition:** Decisions to spend on IT should not be taken lightly – especially in the context of the systems that support and enable core business activity.

However, there comes a time in the life of every business asset where its capabilities and familiarity are outweighed by its costs and constraints, and a shift to a newer generation is appropriate. As banking has become ever more complex, the tendency in most organisations has been to graft on layers of functionality that provides a desired capability, but at the expense of additional complexity and overhead, and with magnified risk of things going wrong. Decisions about expenditure on IT should take a long term view on costs, benefits, opportunities and risks – but in too many cases are overridden by urgency and complacency. *Is your organisation's IT budget too heavily biased to sustaining systems that should be replaced? Are the spending decisions you make today increasing the cost and complexity of your systems in the future and locking you further out of the opportunity for generational change to more relevant technologies?*

**Performance:** In many industries, but especially now in banks, customers expect continuous uninterrupted service. As the NAB experience shows, it's no longer really a business choice – it's a customer imperative. That means that the window of opportunity for resolving problems that do arise is shrinking, and the importance of avoiding problems is increasing. *Do you have a comprehensive and robust testing facility in which you can actively eliminate most problems before they arise in production? Do your testing systems learn from operational experience, with each new operational problem being incorporated into the test suite? Do you have timely and durable access to experts who have in-depth knowledge, skill and discipline required to analyse, isolate and resolve a problem that is debilitating your business? Do you have controls in place to block inappropriate action from non-experts when something does go wrong?*

**Conformance:** The NAB incident has raised a number of questions about the stability of Australia's payments system and opens the door to new questions regarding whether and to what extent there should be regulated requirements relating to the transaction processing aspects of banking systems. But looking deeper, it also appears that NAB has been highly disciplined internally as it dealt with the problem. NAB's communication to stakeholders has been reported as of a high standard and from the right level, though it failed to use all relevant means of contacting customers. There seems to have been little by way of leaks to confuse the picture of what actually went wrong. Action to help customers left without money may not have been extensive enough, but they were also not woefully inadequate. It might just be that NAB had thought about what to do in these circumstances, and acted accordingly. *Do your executives, managers and staff know exactly what to do, what to say, and who to talk to when something goes wrong? Are there conditions in your business*

*license (in whatever form it may take) that may expose your business to consequences if any of your key IT systems fail?*

**Human Behaviour:** Until the birth of the internet and highly consumer oriented IT, many people were prepared to make allowances for the unreliability of information technology. Nowadays, the average consumer, and indeed many people working even in quite high levels of business, see information technology through their experiences with home computers, game machines and so on. They have little patience and quite advanced expectations about the performance and capability of IT, which is not moderated by appreciation of the complexity imposed by scale, regulation, security and so on. On the other hand, people who work in IT roles have a track record of "trying to help", acting outside their boundaries in order to overcome minor problems and to generally be helpful. Unfortunately, without appropriate training, these actions can result in compounding of problems. *Do you have a clear understanding of how your stakeholders will behave if you experience a significant IT based business disruption? Do you have proven strategies and protocols for dealing with stakeholder reactions in the event of such problems? Do your operational personnel have a clear understanding of what they can and cannot do in response to a problem arising with your main IT systems?*

## Learning lessons – the Qantas file

The lead for a story on the NAB problem on the Australian Financial Review website says: *"Top executives at National Australia Bank could be moved after the bank confirmed it would undertake an extensive investigation into how a software glitch on its ageing computer systems left many of its 4 million customers without access to their money for almost a week"*.

Thorough investigation of cause is essential when untoward events put human life at risk, as in the case of aviation, and it may be that the type of outcry following events such as experienced by NAB

The aviation industry has very highly developed protocols for dealing with serious breakdowns. These protocols came into effect on November 4<sup>th</sup>, when the number two engine of a near-new Qantas Airbus A380 exploded just six minutes after take-off.

There will be many discussions of this incident over time, and it is not the purpose of The Infonomics Letter to provide an in-depth analysis.

Notwithstanding, there are some valuable points to be made:

- Investigation of the incident is highly transparent not just to the aviation industry, but to the general public. The Australian Transport Safety Bureau,

for example, has maintained a [running log](#) of major steps in the investigation.

- Every element of the failure and its immediate consequences is being rigorously analysed. There are several [amazing photographs](#) available, showing damage to the aircraft and evidence of the rigour of the investigation.
- Virtually immediately after the aircraft landed and the damage had been visually inspected, a world-wide directive was issued grounding all A380's with the Rolls-Royce Trent 900 engines until the engines had been inspected for possible related problems. This procedure would have contributed greatly to the rapid identification and confirmation that leaking oil had indeed caused an undetectable engine fire that subsequently caused critical engine components to disintegrate.
- Despite multiple instances of serious damage, the A380 was still fly-able and landed safely. Recent estimates put repair costs for the aircraft alone at \$70 million.
- There were five pilots on the aircraft – where the normal Qantas crew for long haul flights involves three pilots. The extra two were there to sign off on training and competence of the primary crew. During the incident, all five were extremely busy, but benefitting from the routine extensive training of Qantas pilots, they were able to divide tasks among themselves and concentrate all efforts on the critical need to land the plane safely.
- Although other A380 operators resumed normal operations after completing inspections, Qantas kept its fleet grounded for almost three weeks, and insisted on several replacement engines being fitted. They maintained a highly conservative stance, and are avoiding using the A380s in circumstances which require maximum take-off power, this mitigating further the possibility of a second failure. Qantas will be waiting for a definite assurance from the engine manufacturer before resuming full operations.

So how does this translate into the questions to be asked of the NAB incident? Consider, for example:

- *Will NAB's investigation be transparent and provide confidence that the cause has been properly understood and that all necessary corrective action has been properly completed?*
- *Should banking systems (and other "lifestyle critical" systems) be designed in such a way that they are highly resilient to failure, and if so, at what cost?*
- *Are there enough experts available to deal with a serious breakdown, and are regular staff sufficiently well trained to take appropriate action when something goes terribly wrong?*
- *If NAB uncovers an underlying flaw in technology sourced from a third party (whether computer equipment or operating system or business application), will the relevant vendor take*

*responsibility for in depth assessment and remedy of the flaw, and will the risk be adequately communicated to all other customers using the same potentially flawed technology?*

- *Will NAB be introducing additional precautions such as extra test cases and stronger controls to limit the possibility of a similar incident in the future?*
- *Will other financial institutions, and other organisations which are highly dependent on IT, seek to learn from the NAB experience and take steps to assess their own risk and to introduce precautionary and preventative measures?*

## Reinecke echoes Gershon

Just over two years ago, British government efficiency expert Sir Peter Gershon delivered his report on the Australian Government's use of IT. Gershon's finding was blunt – that the Australian Government had weak governance of IT. As a direct result of this weak governance, the Australian Government was inefficient in its use of IT, with what he called Business as Usual Expenditure (BAU) too high and a poor record of success in using IT to transform and improve the machinery of government. Gershon said that improvement would require a substantial and sustained change in culture, particularly at the top of the Australian Public Service.

While the Australian Government nominally accepted all of Gershon's recommendations, and went ahead aggressively to begin implementation, it was soon clear to an interested arm's length observer that the implementation would be focusing not on the full set of seven recommendations, and not on the culture change, but on the more technically specific measures required to achieve a significant one-off reduction in BAU expenditure.

An opportunity for Infonomics to provide advice on governance to one government agency during late 2009 and early 2010 eliminated the arm's length restriction and delivered confirmation that there was little, if anything being done to advance either of the first two recommendations delivered by Gershon – to improve pan-government governance and to improve agency level governance of IT.

Subsequently in August 2010, the government announced that the 50% of BAU savings intended for reinvestment were now to be used in non-IT initiatives. The grape-vine indicated that the calibre of reinvestment proposals was so weak and technology focused that there was really no point saving the money for IT enabling purposes.

Gershon recommended an independent review of progress and this task was duly assigned to Dr Ian Reinecke. Reinecke consulted industry and government personnel to form his view of the status of action on the Gershon Report. His [report](#), dated

June 2010, but only released during November, essentially says that implementation to date has focused principally on technology and expenditure issues, and has delivered no discernible improvement in the essential issues of top level governance and leadership.

That's not a surprise, but it should be a matter of considerable concern. The gap identified by Gershon and now reconfirmed by Reinecke is one of vision, strategy and leadership. Without highly effective governance arrangements at the top to set the vision for the Australian Government's use of IT (as an enabler to the most effective, efficient and acceptable delivery of government services to the nation), there can be no expectation that either spending cuts are properly targeted and appropriate, or that the most appropriate mix of initiatives and the most appropriately structured IT-enabled capability development initiatives will be undertaken.

It's not hard to understand how the current situation has arisen. Truly effective pan-government governance of IT, with appropriate leadership at a ministerial level and a diligent translation of vision into strategy at the secretaries' level requires, as Gershon identified, a significant change in culture. It requires:

- a major reorientation on responsibility for IT, with significant take-up of responsibility by government business leaders and an equal relinquishing of responsibility by government technical leaders;
- a new approach to developing vision and strategy which goes beyond paving established paths with new tools, to radically redefine the machinery of government and in doing so change the boundaries of the traditional fiefdoms;
- a new approach to structuring and conducting IT investment initiatives so that effort is focused on delivering the complete systemic change, rather than just on delivering the technology;
- a new attitude to performance measurement for government use of IT, focused on achievement of transformational objectives for new use of IT and effective service delivery in the mainstream activity of the machinery of government;
- a new approach to conformance, elevating the focus from low level detailed policy to higher level principles that guide strategic, tactical and operational decision making, and vastly improved use of standardisation tools such as reference architectures; and
- careful management of the change in culture, recognising that the human impact of such change can be significant and requires diverse, tailored support arrangements.

Underlying the change that is required is a clear and unequivocal need for education. Neither Reinecke nor Gershon specifically identified education as a requirement, but the need should be obvious. Education is a key enabler of change and both have

identified that there is a considerable need for significant change in governance of IT. What was confounding in the early wake of the Gershon Report was the absolute disdain for specific education on the ISO 38500 approach to governance of IT by both government and industry. AGIMO expressed the view that it was already sufficiently familiar with the standard and needed no further insight. When the Australian Computer Society offered a one-day class on ISO 38500, there were zero registrations from Canberra personnel. And while the Australian Information Industry Association created a "governance focus group" as part of its "Gershon Task Force", the focus group never convened even in a distance-mode.

The lessons from Gershon and Reinecke may be addressed to the Australian Government. But they apply much more widely. Governments and businesses all over the world should recognise the value in directing and controlling their use of IT from the highest levels, ensuring that the strategic opportunity of IT is exploited as and when appropriate, and that inappropriate use of IT is avoided.

In Australia, as the Reinecke Report is digested, it's time for us to get serious and undertake the significant cultural and behavioural change that Gershon specified, and the first step in any change is education, for all players.

## Seminar on Governance

Understanding governance of IT and how organisations go about adopting new arrangements for governance of IT is a key theme for research being conducted by a joint high level team of management researchers from Monash University and Deakin University. A seminar conducted in Melbourne at the end of October provided an opportunity for an audience of around forty five from academia, business and industry to see output of the research to date and hear views of industry specialists. Here's a very brief summary of the proceedings:

- *Challenges facing Australian businesses with respect to IT investments and governance issues (Mark Toomey, Infonomics Pty. Ltd.)*

Problems with IT have significant impact on performance of organisations, and the process oriented frameworks for "IT Governance" do not address the key problem – which revolves around behaviour of people and the organisation. Planning, building and running a modern IT-enabled organisation requires a symbiotic relationship between business leaders who define the "demand" for IT and IT leaders who provide the "supply" of IT. Implementation of change requires a deliberate focus on progressive transition of entire business systems, where IT

may be the enabler, but implementing IT-enabled change requires considerable work on the people, process and structure elements of the organisation. Effective governance of IT as defined in ISO 38500 can only be achieved when governance is properly integrated with the corresponding management systems, and with effective, well informed executive engagement, as is normally the case with governance and management of assets such as finance and human resources.

- *Governance of IT and SMEs (Mike Rich and Darrel Weekes, Attaché Software)*

Small and medium organisations have underinvested in IT since Year 2000, and are at risk of unknowingly limiting their business. Yet while the IT they use may be outdated, of greater concern is that many organisations are not taking advantage of the capabilities in the software they do use. In an effort to advance the performance and capability of SMEs in their chosen markets (particularly Australia and New Zealand), Attaché Software spent three years developing its Business Improvement Guide (the BIG). The BIG is not focused on any particular business management software suite, but does highlight the capabilities that should exist in any business software and should be used by business owners and managers to advance the performance of their organisations. Attaché Software believes that IT supply organisations have a frequently undelivered obligation to help their customers become better users of IT. They also believe that business leaders must take responsibility for their own success and performance, and this includes being responsible for ensuring that they are making best use of appropriate IT systems.

- *Change Management: a CEO/CIOs perspective (Ernest Stabek, Principal SIP)*

Change Management is a term used in many areas of business and often misunderstood due to the complexity of what is involved in managing behavioural change. When engaging in discussions with CIO, change management professionals and business executives alike the key messages can change depending on whether the topic is organisational change or functional redefinition, change enabled by some form of ICT automation or alternately workforce transformation aimed at extracting efficiencies by simply reconsidering the way we do things.

Change managers often refer to change as impacting on people's lives and thus triggering various behaviours. CIOs on the other hand look at Change as a process of transitioning the organisation from a current state to a future state. For business executives, change is often viewed as

an essential element of innovation and survival to achieve desired strategic outcomes be that profit or not for profit.

In all three perspectives the key challenges for change management include getting people to buy into the change vision, finding the right leadership and critical mass of change advocates within an organisation and knowing when to time a switch in leadership styles to maximize the effect of intended changes.

Change management now and in the future could be defined as imbedding behavioural acceptance. If we can let go of our individual vested interest we can embrace change for all the right reasons and work collaboratively to achieve major shifts in thinking on how we can improve the business models for the future to minimise waste and embrace creative innovation in all that we do or aspire to be.

- *International Survey Results (Mark Toomey, Infonomics Pty. Ltd.)*

An international survey conducted by Infonomics in early 2010 collated views on governance of IT from 75 board directors, business executives, IT leaders and consultants. Governance of IT does involve evaluating, directing and monitoring the current and proposed future use of IT. It involves overseeing preparation of plans for use of IT, overseeing delivery of business change enabled by IT and overseeing ongoing operational use of IT and it requires a set of management systems that are fit for purpose and appropriate to the nature of the organization. The management systems must be clearly defined, complete and auditable, engaging both business managers and IT managers and must provide the information needed for effective governance. However in many organisations, executive management lacks the knowledge and skills to make sound judgements regarding use of IT. 60% of boards don't have effective oversight of IT and even more lack the skills to provide effective oversight.

Achieving business outcomes is the key measure for success of IT projects, and this is a clear responsibility of business managers, but only one quarter of organisations have a strong track record of success in this regard. Operationally most organisations are critically dependent on IT, but less than half of organisations give executive management evidence that operations are sustainable. Executives fully understand the value and risks of their IT in less than a quarter of organisations. Effective governance of IT is a definite strategic advantage, but effective governance exists in less than 5% of organisations.

- Case Study I on IT Governance (Paul Couchman, Deakin University)

A major non-hospital health services organisation is heavily dependent on IT, focused on supporting the front line workforce. IT is a key factor in a growing competitive market, with multiple projects and an imperative to manage the relationship between human factors and technology.

To improve coordination and management of IT-enabled change the company has moved to more tightly integrate business and IT strategy, and to use formal frameworks (PRINCE2 and ITIL) for project and change management respectively. The board engages strongly on governance of IT, focusing on direction and risk, and is supported by active external and internal audit. A continuous improvement culture is important, as is pragmatism regarding what can be done. Proposals for investment in IT must be business outcome focused. Governance arrangements can effectively evolve over time, and can benefit from the guidance in ISO 38500.

- *Organisational behaviour relating to IT Governance (Kylie Prince, registered Organisational Psychologist)*

Can business drive exploitation of Information Technology?

Organisations function as systems within frameworks of larger societal, political, economic, and environmental systems. Systems thinking deals with the connections between all systems and the influence they have on each other. Ongoing systems change influences business practices, structure, resources, management and leadership behaviour. Change influences people's attitudes, beliefs, behaviour, and perceived needs; influences stakeholders; and influences communication and information flow.

Information Technology plays a fundamental role in the organisation's information and communication flow. New experience and the better availability of information supersede old expectations and consequently progressive change enables the organisation to ascend to higher performance levels.

Traditionally governance of Information Technology has been considered the function that aligns Information Technology and business. But, understanding that Information Technology keeps information and communication flowing within the organisation; the governance of Information Technology should now be considered as the leadership function that aligns the entire organisational system with evolving availability and capability of information technology.

Business currently perceives Information Technology as a tool and underutilises its full potential. However Information Technology can transform business operations and consequently the entire organisational system through appropriate governance of Information Technology and managing required change.

Visual intelligence is the ability to take an overarching view of the entire organisational systems, and the entirety of the external environmental systems. When leaders lack skills required to visualise and understand the bigger picture, organisations can experience problems with managing change.

Effective governance of Information Technology requires visual intelligence. Executive officers and board of director functions need to develop this capability to enable spatial recognition of appropriate information technology opportunities and advancement of evolutionary change. Managers high in visual intelligence will effectively understand the whole-of-business-system transformation relative with the bigger picture information revolution, new technologies, and adapting business and workforce practices; essential for unleashing the potential of Information Technology.

Many organisational managers lack spatial capability required to step back and visualise the big picture vision of an organisation, where they have been, where they are going, and how they will achieve their goals. This results in lack of ability to conceive the role Information Technology actually plays with the business system.

- *Case Study II on IT Governance (Carla Wilkin, Monash University)*

A large not-for-profit healthcare organisation faced challenges with effective allocation of funding for IT projects. The CIO recognised the need for a unified executive management view on allocation, leading to creation of an "IT Governance" Committee and establishment of a CIO-CEO direct reporting relationship. A Project Management Office was established to enable a portfolio management approach to selection and conduct of projects. Effective use of the organisation's intranet enabled ready access to the new governance arrangements and small incentives were used to promote participation.

It was noted at the end of the presentation that this case study actually focuses on a management system which would be one part of an overarching approach to governance of IT.

• 4.30 pm *Open Discussion – Where to Next?*

An all-in discussion of key points arising from the seminar, how to advance the cause of effective governance of IT, and further research opportunities resulted in the following list:

- ✓ Continuing need to educate leaders;
- ✓ Tailor message for peak bodies;
- ✓ Identify the best strategies for how to best communicate Governance of IT and for putting it in place;
- ✓ Involvement from users of IT in defining the governance of IT;
- ✓ Develop clearer understanding (definitions) of what terms actually mean i.e. "IT Governance", "Governance of IT" and IT Management;
- ✓ Look at sustainability cases and map these, looking at the lessons learned;
- ✓ Put a \$ value on Governance of IT;
- ✓ Need more frameworks for Governance of IT;
- ✓ Work across different industry sectors – government, public, private etc.;
- ✓ Get universities to undertake Governance of IT and use it as a case study;
- ✓ Board evaluation – inadequate focus on the governance of IT in board level evaluation. Many boards are dismissive of this topic, but change is inevitable – boards can no longer ignore IT.

No doubt these discussion points, including contributions from audience members representing a wide range of stakeholders including board directors, executives, consultants and academics, will evolve into a stimulating program of work during 2011 and beyond.

## **New Opportunity to Improve**

This week has seen election of a new government in my home state of Victoria, and a new opportunity for a government-wide improvement in governance of IT.

Victoria's track record of success with IT-enabled change has been mixed, despite development of some very useful management tools. My view, fuelled by direct exposure to some initiatives and conversations with numerous people involved in specific initiatives, is that fundamental flaws in governance prevail and cannot be fully overcome by establishment of yet more procedurally focused management systems. Rather, Victoria needs to recognise the individual and organisational behaviour issues that frequently result in cost overruns, late delivery and sometimes outright failure of IT investments.

Fundamentally, the governance issues pointed out in the Gershon Report on the Australian Government's use of IT also apply to the Victorian Government's use of IT. It will be important now for the new government to introduce effective ministerial level oversight of IT, and this task should be considered an important one for Cabinet. Ministerial oversight should be accompanied by clear and unequivocal assignment of responsibility for effective, efficient and acceptable use of IT to Department Secretaries and other agency heads.

## **Recent/Coming Events**

It's been quiet in October and November, with no new events on which to report. December in Australia is traditionally not a month for major events as everybody prepares for the Christmas and summer holiday season. However, there are two items for the calendar:

Melbourne, December 3: The EA Networking Lunch. I will speak about the directions for Infonomics in the coming year to a diverse group of business executives and consultants. If interested, please contact me for more details.

Sydney, January 20: Dimension Data Learning Services Breakfast briefing. DDLS will be inviting a select group to a briefing on governance of IT.

## **Planning 2011**

One of the central pillars of Infonomics activity is building awareness, understanding and skills in governance of IT and ISO 38500, for directors, business leaders and IT specialists. The Infonomics education program is continually evolving, includes classroom, conference and open access events, and is frequently organised in conjunction with business partners operating around the world.

As 2011 dawns, there are pointers to strengthening economies beginning to drive new investment in IT. This should in turn drive demand for insight about how to ensure that IT delivers appropriate value, with acceptable risk.

During recent weeks, I've begun exploring prospects for delivering education about governance of IT in South America, Canada and the UK.

My preferred approach is to work with partners in each region where I deliver education, sharing the cost and risk of running classes. I work with professional organisations, universities and with companies that have the credibility and reach to attract an appropriate audience.

If you would like to explore the possibility of having me speak at a conference, or deliver an ISO 38500 related training event, or both, please [contact me now](#) and let's get something on the planning agenda.