The Infonomics *Letter*
Plain Language about Corporate Governance of Information Technology
April 2009 Edition

Brave New Worlds

Australia has decided to build a new "National Broadband Network", or NBN. The decision, which came as a surprise to many, has been discussed in the national and industry press at length. At around $42 billion, it ranks in money terms as our largest ever nation building project, and it has certainly generated excitement to match. But what is the project really all about? How will we recognise and measure success, and who is responsible for that success? What could go wrong, and how can we avoid the dangers? In "Australia's Great New Adventure" we explore the NBN from a governance perspective.

One particular aspect of the NBN deserves to be brought into focus for national debate right now. It is possible through intelligent design and effective use of well-proven technologies to make the NBN a much safer vehicle for access to the internet, effectively eliminating viruses, hacking, spam, phishing and other such problems. Of course, such benefits come at a price – a price which some may perceive to be an unacceptable loss of personal freedom. The opportunity, the issues and the precedents are discussed in "Making the NBN Secure".

Closely related to the NBN is the phenomenon commonly known as Web 2.0. Along with that, we are seeing the emergence of more IT buzzwords like "Cloud Computing" and "Software as a Service" (SaaS). As with the NBN (do all these new acronyms ring a warning bell?), the press, particularly that which is focused on IT is full of excitement about these new ways of delivering information technology. But in the excitement, are we missing something? In "The Path of No Fear", we explore some governance issues around these new resources.

There is strong interest in the ISO 38500 approach to governance of IT. In recent events, I have delivered a 2 day extended masterclass in Kuala Lumpur and started the ACS "Education Across the Nation" program on Governance of IT in Hobart, Tasmania.

In May, the first one-day class for Frankfurt has been so well subscribed that we are now scheduling a second event. And conversations are taking place with prospective partners regarding delivery of ISO/IEC 38500 education and other resources in many parts of the world.

And finally, the Infonomics Shop is open for business, enabling you to purchase and download a range of Infonomics publications.

Kind regards,
Mark Toomey
27 April 2009.

Australia's Great New Adventure

"Without a first class system of interstate highways, life in America would be far different --- it would be more risky, less prosperous, and lacking in the efficiency and comfort that Americans now enjoy and take for granted. People would be crowded into more densely packed inner cities, intercity travel would occur less often and be more cumbersome; freight charges would be higher and, as a consequence, so would prices. Vacation travel would be more restricted".

These are the words of Wendell Cox & Jean Love in their report: "THE BEST INVESTMENT A NATION EVER MADE: A Tribute to The Dwight D. Eisenhower System of Interstate and Defense Highways".

The Internet has been termed The Information Superhighway. I first encountered the term in the mid 1980's, when it was used in a report by the consulting firm I was then joining – DMR. The DMR report looked into the opportunities inherent in the emerging phenomenon we now know as the internet, and followed an earlier landmark study into the then very futuristic concept of convergence for text, data, image and voice. Only twenty years after those reports, we were all accustomed to life on the internet – a life transformed by You-Tube, Myspace, Facebook, Salesforce.com, Amazon, Google and so on. But is the Internet a superhighway? For many, the answer would be a resounding "NO". In Australia, it is often slow, expensive, unreliable and dangerous. Why dangerous? Because despite the goodness that it brings to us the internet is also a conduit for many forms of nastiness. Really, using the superhighway metaphor, today's internet in Australia is little more than roughly paved goat-tracks, wending through dark and gloomy woods full of brigands, over harsh and rocky ground, along cliff-faces, and through swamps. Despite the fact that we all use it, and greatly depend on it, the internet in Australia is not really a nice thing.

But now we are at the threshold of a new era – where the internet is transformed into something more akin to the US interstate highway network. Our Australian internet of the future can and should be a key enabler of massive economic, cultural and social growth.

Where much of the press discussion of the NBN has focused on the projected cost of an ultra-fast internet link to the home, and on the impact of losing its monopoly position on the telecommunications giant, Telstra, there have also been some glimmers of light and rational thinking about the opportunity for the future. Among the best of these has been the article in a local weekly industry e-zine called "The Rust

Report" by Australian Industry Group CEO, Heather Ridout. In "Backbone of a smart economy", she says:

"An important element to be noted is that much of the commentary on the costs and benefits of the new proposal seems to assume that broadband usage is limited to the Internet, social networking, e-commerce, and entertainment services. In reality the NBN will accommodate provisions for many applications in addition to these sorts of services.

The new NBN will have the capacity to be a multi-service architecture that will enable new industries to develop around areas such as home health monitoring, remote working, smart grids and e-Security. There are tremendous opportunities not only for new products and services but for much more efficient delivery across this wide range of applications of existing services than is currently possible.

Any assessment of costs and benefits of the government's proposed new investment needs to factor these sorts of potential benefits into the equation.

At the same time, before anywhere near the full potential for these for these sorts of benefits can be realised, additional investments are needed. To generate these sorts of benefits, we need not just the physical infrastructure but also the development and spread of an extensive range of new skills needed for the widespread exploitation of the opportunities. This means additional private and public investment in developing consumer, workforce, and business skills."

Heather Ridout's article should be seen as a call-to-arms for Australian governments and business – to recognise the opportunity inherent in this giant leap forward in infrastructure, and to capitalise on it. And because there is such a gulf between the simplistic perceptions of what NBN is about and the enormous nation-building opportunity that it presents, Ridout's article also calls into question the essential issue of governance for the project.

We know that governance of information technology (which absolutely includes communications infrastructure) is an enormous issue for the Australian Government. Less than a year ago, Sir Peter Gershon told us in plain English that the Australian Government suffers from weak governance of IT at the pan-government and agency levels. Over several years, we have seen failure after failure of IT initiatives at federal and state levels, with audit reports telling us of the same litany of problems arising over and over again. For example, the review of the Australian Customs Service Integrated Cargo System reported: *"We have been unable to locate a clear and quantified set of outcomes and benefits expected from the introduction of the ICS",* and *"there does not appear to have been an effective structure or process to direct and control the project, nor to make suitable risk decisions".*

On the topic of responsibility, the report said: *"Customs has had at least 10 bodies responsible for different aspects of the management and governance of the ICS, including the interactions with industry… … These bodies overlap in their responsibilities and accountabilities, and overall the program has no single business owner and accountabilities for its delivery are unclear".*

What are we talking about when we discuss governance of the NBN project? Are we talking about service delivery – ensuring that the NBN delivers the promised accessibility and performance? Are we talking about design and construction – ensuring that the NBN is delivered on time, on budget? Are we talking about portfolio management – overseeing the many tasks that have to be undertaken in order to build the complete NBN? Are we talking about purchasing and sourcing – ensuring that we have the resources and equipment needed to deliver and operate the network? Or is it all about how the NBN is made accessible to retail service providers, and how its reliable operation is assured? In reality, all of these activities are important – but they are only part of the picture. For none of them address clearly the crucial questions that must be addressed to ensure not just that we have an NBN, but that we take the giant stride into the second half of the 21st century that the NBN makes possible.

For a start, we might look at the lessons from the Australian Customs project, and think now about how responsibility should be allocated for the NBN. We should also consider establishing clear and quantified definition of the outcomes we seek as a nation from the NBN initiative.

But we need not dig through past experience for the key lessons they offer. These lessons have already been distilled into the principles for good governance of IT expressed in AS 8015 and ISO/IEC 38500. These standards provide a powerful lens through which we can consider the governance issues and requirements for the NBN.

Responsibility: Who is responsible for the NBN?

It appears that the government will establish a special agency, probably a government business, to oversee the building of the NBN. One imagines that this entity will also be the operator and the wholesale provider to the numerous retail outlets. It is likely that this agency will be seen as, and formally assigned responsibility for the NBN.

But responsibility for delivery and operation is only one facet of responsibility. The builder / operator / wholesaler is hardly likely to develop the new business models, services and other innovations that the NBN will enable. This is the responsibility of Australian businesses. While they should be expected to encourage, support and nurture such innovation by business, Government agencies have their own

responsibilities to take advantage of the NBN in delivering effective, relevant and useful services to the nation. Individuals who use the NBN have a responsibility to use it properly, for proper purpose, and to not interfere in its operation.

Educational and research institutions, together with government and business, have responsibility to develop the innovative ideas and related skills that are necessary enablers to finding and realising new opportunity. Business leaders have a responsibility to recognise the kind of opportunity that the NBN offers, and to consciously factor this opportunity into their strategic planning. Corporate boards have a responsibility to check that management has indeed considered the changing communications landscape.

Organisations that have independent communications infrastructure will carry additional responsibilities as well, to not constrain the value and growth of the NBN, to exploit it to the benefit of their customers and shareholders, to avoid unnecessary redundancy and duplication, and to not engage in the sort of anti-competitive behaviour that has been an unproductive reality for Australia over several years.

Strategy: What is the purpose of the NBN?

At one end of the spectrum, the NBN can be seen as a monopoly breaking exercise, neutralising the absolute power that the major telco has over communications access to the majority of Australian premises. At the other end of the spectrum, the NBN can be truly seen as "nation building", and it is, fortunately, in this context that it is most discussed.

But what does "nation building" mean? Is the strategy merely to establish the world's best and most pervasive high speed broadband communications network? One would hope not – for to do so would stop well short of anything that delivers the tangible benefits to the nation that such an investment offers.

To build on the initial surprise and delight, and to promote the development of ideas, we need to have a clearer, fuller strategy, that is anchored in a vision of Australia in the future. What exactly is that vision? Could it be a vision of a wealthier nation, a leading global citizen, exploiting the power of effectively instantaneous and pervasive communications to devise and deliver service that has been hitherto inconceivable outside the realm of science fiction and fantasy? Could the vision include and go beyond the suggestions of Heather Ridout? Could it include the world following Australia's lead, and the world's greatest innovators choosing to do their work in Australia because this is the nation that best encourages and facilitates innovation?

If we express the purpose of the NBN as merely being to have a great, high speed, high capacity broadband network, we will be selling far short the opportunity. But if we wait too long to establish our vision and strategy, we may well end up with nothing more than a fast network that we do not have the wherewithal to use effectively. We need the vision to drive the strategy, and the strategy needs to be multi-faceted, so that in conjunction with the network, we build the capabilities and resources to exploit it fully.

Acquisition: Is the decision to go ahead with the NBN a valid one, based on sound research, and with a compelling business case?

As said before, one of the drivers for the NBN is certainly the elimination of a monopoly obstacle to progress. But this in itself probably does not justify the price tag. Is there more to the opportunity?

Certainly, the federal government has considered a partial solution – one that offers "fibre to the node" rather than "fibre to the premises" at a significantly cheaper cost. But that option was still hostage to the monopolists control of the "last mile" of copper, and thus at risk of compromise. It was also limited in its performance to levels that are merely equal to international competition, rather than being a quantum leap ahead. Thus, the additional spend is presented as being justifiable in the context of the opportunity that it presents.

But if the strategy for the NBN needs to be more than merely building the world's most pervasive, most advanced and most powerful broadband network, so too does the acquisition process need to look at more than the engagement of contractors to supply and install the equipment. The investment decision needs to look dispassionately at the effort required in other contexts to ramp up and nurture the exploitation of the new infrastructure. It needs to look at and guide action on a wide range of policy instruments that together provide the building of complementary capabilities.

Performance: How do we ensure that we get the necessary value from the NBN?

Building on the points made under the Acquisition heading, it should be clear that performance of the NBN should be evaluated in terms much wider than the rate of rollout, the actual bandwidth delivered, and the reliability of the service.

To start measuring performance of the NBN in the most appropriate and objective terms, we need to have established clearly what the strategic intent is, aligning the measures of performance with the definition of the outcomes that the strategy should deliver. And in addition to measuring the performance, we need to understand the enablers of that performance, and do the things necessary to ensure that those enablers are all in place. We need to measure not only the end result, but the journey – for it is in elements of the journey that the true value will be created. Drawing from the lead provided in Heather Ridout's article, we should be looking at performance indicators such as the creation of innovative new businesses and services from

established businesses. We should be looking at the migration to Australia of offshore businesses and specialists who will help drive the innovation. We should be looking at the rate of submission and approval of innovative research and development proposals that contribute to the long term goals, and we should look at the supply pipeline for suitably skilled people who will help devise new ideas and transform them into reality.

Conformance: What rules will be needed to maximise the value and protect the integrity of the NBN? Who should set and enforce the rules?

It seems fairly clear that the NBN is to be established as a wholesale service, to be resold through a wide range of service providers, service integrators and value adding organisations. This structure in itself will require establishment of clear rules, protocols and processes for the effective ongoing operation of the service. But there will be other rules not focused on front-line, day to day operation that will also be important. The relentless march of technology evolution will ensure that the early deployment components are different to the equipment used in later deployment stages. To remain competitive – especially in the context of placing and keeping Australia at the leading edge of the world's broadband empowered communities, the network will need to undergo a constant program of renewal and updating. With no competitive force, there will have to be another driver for this renewal. With the NBN architecture based on a mix of fibre, wireless and satellite, there will need to be clear rules to guide decisions about when and where fibre is rolled-out to replace the slower forms of carriage.

Another significant area for discussion in the context of conformance is the topic of security. In fact, this topic is so significant that it gets its own discussion elsewhere in The Infonomics Letter.

Human Behaviour: What aspects of human behaviour must we consider in delivering the NBN?

Beyond all else, the ultimate decider of whether a technology enabled change is successful is the decision by people to take up and extract value from the change.

If all that Australia does with the NBN is use it to replace the current offerings for internet browsing and file downloads, the investment will have been a failure. But if we see the opportunity taken up to develop new opportunities, new products, new business models, we have the makings of a success.

There needs to be careful consideration of the behaviour of people as individuals and as communities – where the communities take many forms, including businesses, regulators and so on. People and communities need encouragement for to step out and exploit the opportunity. Students should be encouraged to develop relevant skills, just as researchers should be incentivised to explore possibilities. Entrepreneurs may require some prompting together with a supportive regulatory framework, seed capital and other resources to help them build new products, services, business models and new value. Regulators must be given clear instructions on the desired outcomes of the initiative, and the behaviour they exhibit in their roles as supporters and guardians of value and propriety. All of this must occur within a medium to long term view, and avoid the pitfalls of short-termism, such as punitive pricing for early adopters and failure to develop important legal frameworks.

Without doubt, Australia's proposed National Broadband Network offers a gigantic stride into the future for the nation and its people. Realising the value involves a great deal more than simply purchasing switches and laying cables. The initiative cries out for an effective approach to governance and thereby presents itself as a world-leading opportunity for adoption of the world-leading standard for governance of Information Technology that was also developed in Australia.

Making the NBN Secure

Imagine for a moment the possibility of your business and home internet service today being free of spam email, phishing, hacking attacks, viruses, trojans, worms and the myriad of other nasty aspects of internet use that cost us so much money and time, and put us, our businesses and our families at risk. Can such a scenario be possible?

The internet of today has a design characteristic that is both a key enabler to its rapid take-up and the genesis of a burden that we all carry. The internet design embraces the principle of anarchy – where there are no rules about what people may or may not do, and no way – or at least very limited ways in which any rules can be enforced. In its earliest incarnation, the internet was much more of a closed environment in which the concept of anything but benign use was probably far from the minds of the designers. When the internet expanded beyond the closed environment, and having caught the public imagination, expanded greatly, it was too late to go back and re-engineer it to be secure and safe.

Compare the internet to the telephone system. In most parts of the world, both fixed line and mobile telephone systems have the ability to display the originating number for a call on the recipient's phone – the technology is known as Caller-Id. Even when caller-id is not enabled, the underlying technology of most telephone exchanges allows calls to be traced. What this means is that there is a straight-forward and readily available means of locating miscreants who would use the telephone network for improper purpose. While the possibility of detection is not a deterrent to some, it does mean that many who might

be inclined to casual misdemeanour do not go down that path persistently. It also means that there is potential to identify, apprehend and prosecute those who are persistent offenders. A robust, well tested and evolved legal framework spans the use of these technologies to limit the opportunity for abuse. Thus, in Australia, call tracing is accessible only to properly authorised agencies. Phone taps generally require authorisation from the judiciary. Call recording is often allowed only with agreement and recording pips. Telemarketing has been controlled through establishment of the "do not call" register.

Can we move the internet to a similar level of security? From a technological perspective, the answer is a simple "Yes". Indeed, many organisations that run private communications networks (intranets) use commonly available technology to make their internal networks robustly secure.

The NBN presents Australia with a once-in-a-lifetime opportunity to move from the anarchy and security compromises of the original internet to a safe, secure, respectful communications situation. Without need for monitoring the activities of any individual, the NBN can provide an environment in which all data, regardless of form and content, can be traced to its NBN entry point. That capability means that data arising from inappropriate and malicious intent would be traceable to its source, and as a result, the perpetrator can be held accountable.

We can build the NBN as an independent, parallel network to the existing conglomeration of twisted copper, cable, fibre and wireless joined up by switching systems of varying ages, and conforming to a multitude of compromise based standards. The NBN can interconnect to the old networks using gateways, which can be relatively few in number, and equipped with powerful tools for protection so that nasties cannot traverse the boundary. The premises connection points for the network can be intelligent devices that positively identify themselves to the network's control system, ensuring that only properly authorised and properly configured connection points can participate in the network. These connection points can wrap all of the data they carry with control information that allows, subject to proper legal controls, positive identification of the source and destination for every piece of data, as well as tracking for audit and enforcement purposes.

Rather than blocking any individual's access to inappropriate services, and rather than actively preventing any specific use of the NBN, such an approach removes the assurance of anonymity that pervades the current internet, and in doing so creates the enforcement stigma that is an essential element of steering human behaviour. Put simply, the likelihood of discovery would be greater and would in its own right discourage much of the negative behaviour of today.

Of course, the prospect of discovery does not discourage the determined miscreant. But the same technologies that would make the NBN secure can also provide evidence, and control. Again subject to appropriate legal controls and perhaps judicial oversight, traffic carried on the NBN could be tapped, just as telephone calls can be tapped, and the data could be recorded for use in evidence. The technology that enables positive confirmation of the source of data can also provide positive proof that recorded data is precisely as transmitted, and has not been manipulated in any way.

Some may say that making the NBN secure is insufficient, as it would still need to connect to the old national communications networks, and to the international networks. This is exactly correct, and the old networks, with much lower levels of control, can still be sources of many problems. But by designing the NBN with well-controlled interconnects, the opportunity arises to both discourage use of inappropriate resources and to actively block others. Classical spam is one instance. Rather than spam being blocked at the ISP, or even at the end-user's computer, it can be blocked at the interconnect – never entering the network in the first place. Websites that are known for "Phishing" can be blocked and made inaccessible at the interconnect as well. And anybody foolish enough to establish an inappropriate site on, or to send spam via, the NBN would quickly discover that the source is traceable and that robust evidence can be gathered speedily.

The vision of a secure NBN described here is just that – a vision. But it is also an eminently attainable vision, achievable at very low cost if the design work is done now to build it into the fabric of the NBN.

It is also a vision that may generate fierce resistance. Many will not want the NBN to be secure to the extent that is proposed here. The extent of security needs to be established through properly informed public debate, and the debate needs to start right now. We can expect resistance to come from three main areas: those who would be prevented from engaging in inappropriate behaviour because of the security, those who for reasons of principle have no trust in any "big brother" capability to monitor and regulate the behaviour of the citizens, and from those who, while in legitimate businesses, profit from the problems in the current communications environment – such as companies specialising in internet security and anti-spam resources.

The Path of No Fear

Last month we discussed why (not whether) the first generation of "IT Governance" has failed. We noted that in most respects, the "first generation" of IT Governance has focused on the supply of information technology by the in-house IT department and by the major outsource IT providers.

A perception that has developed in many organisations is that IT Governance obstructs achievement of business goals. Business users have sought ways to bypass the main IT supplier in order to achieve their goals. Twenty years ago, this was done using personal computers and shrink-wrap software, with business users operating outside the mainstream of IT professionals to build functionality that the IT department either could not, or did not want, to deliver.

Today the new opportunities for speedy delivery of business capability are Web 2.0, Cloud Computing, and Software as a Service (SaaS). The beauty of these technologies is that they are accessible to and useable by people who have relatively little knowledge of technology. Their perceived virtues of speed of establishment and low cost are in many cases absolutely true – and many organisations have benefited. For example, Infonomics uses a Web 2.0 service to manage delivery of The Infonomics Letter. At a nominal fee, the service provides comprehensive management of the mailing list, automatic scheduled deliver of announcement emails and comprehensive statistics that help us to understand who is reading The Infonomics Letter.

As these new generation tools become more sophisticated, business leaders (and maybe also IT leaders) would be asking themselves whether and to what extent they can and should use them to underpin their business. It's a fair question, but one that has many issues to be considered.

In an internally controlled IT environment, organisations can have visibility and control over a number of essential aspects of how they use IT. Do they have the same control, and do they need the same control, when they are using commercial web 2.0 services? Anecdotal experience suggests that for some, Web 2.0 may be far from appropriate.

For example, web-based customer and sales management systems give users a powerful portfolio of tools for managing customer relationships. They can give small organisations access to capabilities that would otherwise be unaffordable. But what about when one pocket of a larger organisation's sales team moves onto such a service in frustration over lack of functionality or service from the corporate solution? Immediately, the company's picture of its customer relationships is fragmented. Some of the data is outside on the web. Some of it is on the main system, and unless somebody has been very clever, there is probably no integration of the data to enable a complete picture.

A well-designed and built corporate computing environment has links that integrate the various systems so that there is a complete, accurate picture of the entire company's business. These links typically ensure that data is accurate and consistent, with generally a single master copy of each main set of data – customers, accounts, supply, inventory, sales and so on. Indiscriminate use of narrowly focused Web 2.0 resources can mean that such integration links are not available, leading to multiple copies of key data that can rapidly become inconsistent. Establishing which data is correct is one of many challenges that can emerge.

Corporate systems environments often include strong controls over access to, and preservation of data – which may be trade secret, subject to privacy controls and sensitive in many ways. What controls exist in the Web 2.0 worlds? We hear regularly of data being exposed inadvertently from such sites. Are the risks acceptable?

It's not just the sales type applications. We hear regularly of issues for organisations where employees are using tools like facebook and twitter in ways that create risk to corporate profile and performance.

What is interesting about these phenomena is that in many cases, the people involved have little or no formal training in respect of information technology. They are able to use the accessible functionality, but they have little awareness of the pitfalls. In essence, when they use the new generation user-accessible resources, they are taking the "path of no fear". They are unaware of the dangers, and take few, if any precautions to head the dangers off.

The first generation of "IT Governance" focused on supply of the IT by the IT service provider and did not cope well with how technology evolution allowed the supply to "escape" from the IT department. The second wave, for which ISO/IEC 38500 is the spearhead, focuses on the use of IT by the organisation, and positions governance of IT as something that applies equally to the IT that is delivered by internal and outsourced IT departments and to that IT that is acquired through new sources via the web.

Learning about ISO/IEC 38500

Infonomics can arrange a 25% discount for subscribers to The Infonomics Letter at the BSI British Standards conference on governance of IT in London, UK on May 20. Contact Infonomics for the discount.

The 28 May full day masterclass in Frankfurt is heavily subscribed, and we are now offering another session on 27 May. Click on Serview – the Business IT Alignment Consultants for information and to register.

Click here to see more details on forthcoming education events.

The Infonomics Shop

At last we have the shop operational. Click here to browse the reports and books available, and to purchase them for download or delivery in hard copy format.