The Infonomics *Letter*

Plain Language about Leadership and
(Corporate) Governance of Information Technology

March 2011 Edition

Staying Safe

Welcome to the Infonomics Letter for March 2011.

Some time in 1978, I attended a conference where several companies were demonstrating software on one of the workhorse computers of the time – a DEC PDP-11. Out of curiosity, I went to one system console and logged on. I didn't need to ask anybody the password – most PDP-11's running that operating system used the password originally set at the factory and nobody at the factory saw any need for different passwords. When the first PC was released, it didn't even have the means to identify different users – let alone keep them separate with different passwords.

In 1987, newly arrived in London, I picked up my ATM card and proceeded to an ATM to reset the PIN. I was horrified that, having entered my old and new PINs, the ATM then checked that I had entered my new PIN correctly – by displaying it back in big digits on the screen. Thankfully nobody was watching. Of course banks have learned a lot since then, and they would never show a customer PIN today. But while banks have learned a few things about information security, one wonders about the greater community. In a previous edition of this Letter I've commented on website operators that, having demanded we set up an individual account with a secure password, then kindly send us a clear text email putting all that identity information out where it can be seen by any errant teenager with the most primitive hacking tools. One mailing list I use very nicely reminds me every month of my user id and password. You can bet that I keep that one quarantined with a fake name!

Recently I wrote about the appalling lack of access control in mobile phone shops run by Vodafone Hutchison Australia (January edition, *More red faces*). Now I find that another phone company demands a strong password for access to customer accounts online, and then requires the customer to quote part of that password when accessing the call centre – with the whole password visible to the call centre operator. Don't they understand information security?

Public disquiet about information security breaches and weak safeguards used by many organisations is now driving strong regulatory and legislative action. The probable high cost of information security in the future may be in part a consequence of organisations failing to take early and decisive steps to direct and control their information security. But while legislation may oblige organisations to pay attention to information security, it can't define how to do the job. So, this month's key topic explores how those who govern organisations can direct and control their information security arrangements. Enjoy!

Mark Toomey 31 March 2011

Governance of Information Security

Press reports of information security breaches are nowadays an almost daily occurrence. If we take a global view, there would be dozens, if not hundreds of breaches reported and discussed every day of the week. Among the headlines noted by Infonomics during March 2011 we saw:

- Stolen BP data a warning for Australian companies
- Aussie ATMs a laughing stock
- Hacker takes off with TripAdvisor's customer email database
- Hundreds to be briefed on hacked security firm's technology
- Play.com warns of customer e-mail security breach
- Warning over Skype security weakness
- High-tech criminals outsmarting the law
- French government hit by spectacular cyber attack
- Hackers hit Gillard, ministers' computers

The above are but a small sample of many cases around the world where criminals are directly, actively and in many cases aggressively seeking to profit by obtaining access to, using or changing sensitive personal, business and financial information.

But guarding against the actions of criminals is only one dimension of information security. Another, increasingly relevant dimension is that of keeping information available and safe from accidental loss or destruction. These headlines illustrate the point:

- Gmail messages vanish for about 150,000
- CIOs warned to prioritise governance and business continuity
- Telstra power fault takes out Australia Post contact centre phones

Governments, businesses and individuals today depend on their information being available to them at any time and from, in many cases, any location. Loss of access, even for short periods, at best causes frustration and inconvenience, and at worst can result in serious consequences for individuals and organisations.

Information Security Risk is not confined to external and technical issues. There are just as many cases where the privacy and integrity of information are at risk due to what might at first be dismissed as benign factors. In Australia recently, a mobile telephone provider was forced to act after being extensively castigated in the press for failing to ensure a proper level of control over staff access to customer records. In Britain, the new Information Commissioner's Office is issuing substantial fines to organisations that are found to have lax data security arrangements.

The message is clear

As our world moves rapidly into the full realisation of the information age, it has become abundantly clear that security of information is a critical matter for every individual, organization and government.

The consequences of failure in information security range from relatively benign and trivial, to extraordinary. The trouble is – what may be benign in one case may be devastating in another case. What may be a nuisance at one level, can create an immense impact at another. Breach of a teenager's email may expose juicy gossip. Breach of email systems used by a nation's top executive may result in draconian international consequences. Exposure of a customer's password on internal systems may enable an errant employee to steal the customer's identity and subsequently access that same customer's information held by other organisations – including banks!

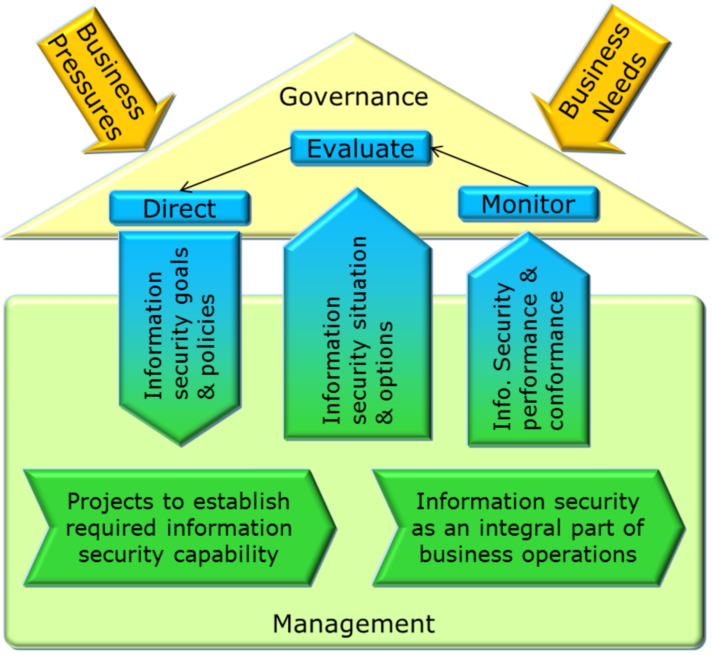
Every individual and every organisation has a duty to protect their own information, in their own interests. Now, every individual and especially every organisation has a duty to protect the information that they hold about others. To neglect this duty puts those others at risk of consequences over which they have no control. Increasingly, governments and other regulatory agencies are recognising the extent of these risks and, in the face of market failure to act appropriately, are embedding the obligations in legislation and enforcing the legislation aggressively.

Oversight of risk is a fundamental element of governance for all types of organisation. Information Security is no longer merely an emerging field of risk – it is well established as a critical and highly active field of risk that must be high on the agenda for every organisation's governing body. The governing body must ensure that the organisation has a sound understanding of the information security risk it faces, on an ongoing basis, that it has appropriate and effective treatment in place for that risk, and that there is an oversight regime that both keeps the information security regime effective, while also ensuring that incidents which do occur are effectively and efficiently resolved.

These obligations of the governing body with respect to information risk map directly to the tasks for governance of information technology described in ISO 38500, the international standard for governance of information technology. As the vast majority of the world's information is stored and communicated using information technology, it is not unreasonable to view the tasks for governance of information security as a subset of the tasks for governance of the use of information technology. Indeed, as one can readily argue that stone tablets, paper, film and so on are merely early forms of information technology (technologies for the capture, storage, processing and dissemination of information), the recommendations for governance of IT in ISO 38500 should guide governance of information security regardless of the medium on which the information is stored.

A model for governance of Information Security

The model for governance of IT presented in ISO 38500 is equally applicable to specific aspects of IT use, as it is to the overall use of IT. Thus it provides an ideal frame of reference for discussing the governance of information security, and can be made quite specific merely by refinement of terminology.


Business Pressures
Business Needs
Governance
Evaluate
Direct
Monitor
Information security goals & policies
Information security situation & options
Info. Security performance & conformance
Projects to establish required information security capability
Information security as an integral part of business operations
Management

* Adapted from ISO 38500

The model shows that:

- The governing body, through management, should evaluate the organisation's current information security situation and options for ensuring that it has an appropriate level of information security
- The governing body should direct management with regard to goals for information security, together with policies that condition decisions management makes about information security
- Management should, as directed by the governing body, put in place the necessary capability and arrangements required to realise the organisation's goals for information security
- Management should fully integrate the organisation's information security capabilities into the organisation's ongoing business operations and should ensure that its chosen information security arrangements are part of the fabric of the way the organisation conducts its business
- The governing body should monitor the organisation's ongoing activities for conformance to the established policies for information security, and should monitor the information security arrangements for efficacy in the context of the established goals and evolving market conditions.

Evaluate Information Security

ISO 38500 says that the governing body for any organisation should evaluate, direct and monitor its use of information technology. It follows logically that the governing body should also evaluate, direct and monitor the information security situation.

As is explained in *Waltzing with the Elephant*, evaluating information security does not necessarily require that the governing body itself undertake a comprehensive assessment of threats and treatments. Rather, it means that the governing body should ensure that management has undertaken such an assessment, and that the assessment is repeated at prudent intervals. The assessment process should ensure that management has a clear and sufficient understanding of the risks and treatment options, and should result in recommendations to the governing body regarding the acceptance of tolerable risk, the treatment of intolerable risk, and any residual risk that cannot be controlled in a cost-effective or practical manner.

Through the work of management to evaluate risk, the governing body should itself be well-informed of the risk to information security. To obtain further comfort and assurance that management's evaluation is appropriate, the governing body should from time to time obtain independent external advice on the organisation's situation. Prudent members of governing bodies, as well as their managers, should also maintain general awareness of the prevailing climate in information security risk, covering both the rise and decline of specific risk categories and sources, and the efficacy of treatment options.

The information and recommendations prepared by management will form the basis of direction provided by the governing body. To assure itself that the direction provided is appropriate, the governing body should rigorously test management's clarity and depth of understanding of the assessment, as well as its confidence in and commitment to the recommended treatments. For example, as information is invariably part of the fabric of the business and is gathered and used in many different parts of the business, it would seem insufficient for all aspects of information security assessment and treatment to be channelled through a sole manager, unless there is obvious and absolute consistency of view across the entire management team. On the other hand, the governing body might be concerned about an assessment of information security and treatment that is distributed across the management team without obvious cohesion on significant risks and treatments.

Direct Information Security

Based on its assessment of information provided by management and, if considered appropriate, from alternative sources, and weighed in the context of market awareness, the governing body should provide clear direction to management regarding the information security goals of the organisation, and the arrangements for achieving these goals. In many cases, the specific direction should be proposed by management as part of facilitating the governing body's evaluation, enabling the governing body to make the key decisions, but avoiding the requirement for the governing body to hold specific skills in information security.

Direction on information security should address a range of matters, including:

- Conformance to applicable laws regarding any and all aspects of information security
- The organisation's risk appetite regarding information security
- Investment in necessary capability to safeguard information security
- Allocation of resources to enable development and ongoing operation of information security arrangements
- Assurance regarding efficacy of the arrangements for information security
- Recording, tracking and reporting of incidents pertaining to information security risk
- Behaviour of the organisation, its personnel and agents with regard to information security
- Behaviour of the organisation and its senior management in the event of a major information security incident.

Monitor Information Security

Criminals and other subversive agents work tirelessly to devise new ways of breaching safeguards that organisations use to fulfil their information security safeguards. It is far from sufficient to simply invest once in an information security capability and treat the issue as resolved. Rather, organisations should maintain awareness of the changing information security landscape and take action as necessary to maintain the desired level of protection as directed by the governing body.

While the capability and impact of criminal behaviour continues to grow, research and many anecdotal events have demonstrated that many of the main threats to information security come from within the organisation (including through outsourcing arrangements). Internal controls and other arrangements for maintaining information security can become degraded over time as a natural consequence of other aspects of organisational change and staff turnover. Thus, organisations should incorporate into their monitoring regime specific elements that will highlight an unacceptable loss of rigour in information security arrangements well in advance of any possible consequential breach.

The precise means by which any particular organisation monitors its information security will vary depending on its circumstances. Regardless, the monitoring arrangements should provide for demonstrating the efficacy or otherwise of the information security arrangements in place, as well as highlighting any significant change in the information security landscape.

Considering that information security incidents can occur with no warning and can rapidly escalate from what initially appears to be a minor infraction to what ultimately may have far-reaching consequences, it is essential that the monitoring arrangements not only provide the governing body with timely awareness of serious situations, but that there is an effective path for escalation so that serious information security incidents receive prompt and comprehensive attention from the most appropriate levels of management.

Principles for governance of information security

As with the model for governance of IT, the principles for good governance of IT expressed in ISO 38500 are highly relevant in the context of information security. When considered in the light of information security, the principles help organisations define the behaviour they intend to exhibit as a whole, and the behaviour that they require of their personnel in respect of information security. In this context, the principles provide a powerful basis for the development of policy, and through policy, a guide to decisions that will be made regarding identification and treatment of information security risk.

Responsibility

Throughout the organisation, there should be clearly understood assignment, acceptance and discharge of responsibility for security of information. From an overarching perspective, the entire organisation must accept that it has operational, legal, ethical and moral responsibilities to maintain adequate security of the information it holds. Within that broad understanding, it is necessary to establish the more specific assignments of responsibility for information security to individuals throughout the organisation.

The mere fact of information being predominantly stored using information technology does not automatically mean that IT specialists are solely responsible for the security of the information. There are many ways in which information security can be breached by personnel far removed from the IT environment, such as careless disposal of printed material, or even making computer screens visible to unauthorised personnel or outsiders.

An effective approach to information security requires a comprehensive approach to responsibility. In most cases, every individual in the organisation will carry some responsibility for information security, while a more limited number of personnel will have very specific and sometimes onerous responsibilities. To avoid overlap and redundancy, it is important that all necessary aspects of responsibility for information security are properly identified, clearly communicated and regularly reinforced. Individuals must understand their responsibility, have the training, capacity and other means of discharging it, and be given appropriate incentives to do so diligently.

Strategy / Planning

Goals set in respect of information security must be achievable and should clearly match the exposure, context and aspirations of the organisation as a whole. The arrangements for maintaining information security must be aligned to the goals, and be both effective and efficient. The resources allocated to achieving and maintaining the desired level of information security performance and conformance must be adequate to the task, not just in normal circumstances, but also when an actual serious information security incident is occurring.

While already a perhaps daunting set of requirements, the above points are often taken only in the context of an information security veneer over an intrinsically insecure information storage environment. But just as multigrain bread is not made by dipping a ready-baked loaf in a sack of seed, achieving truly effective arrangements for information security typically requires a more fundamental attention as an integral part of planning, building and operating the organisation's actual business information systems.

Thus, in addition to ensuring that there is appropriate alignment and resourcing to the external manifestations of information security, the strategy principle should cause organisations to think about how they make information security an integral element of their entire information systems and business systems environment.

Clearly, considering the frequency and severity of "security updates" for much of the software that we use today, there is a dual challenge of first establishing a culture and the necessary resourcing for making information systems intrinsically secure in the first place, and then for overcoming the deficiencies that exist in established technology that may stay in place for significant periods of time (noting that some code in banking systems, for example, is nearing fifty years of age.

Balance is essential in planning and allocating resources to information security. It is very easy, and entirely inappropriate, to over-allocate to high impact, low probability risks because they are "scary", while under-investing in the more mundane, but highly probable risks that can nonetheless cause significant operational, reputational and financial damage.

Acquisition

Decisions to invest in information security capability and arrangements should be made for the right reasons, and in a proper manner.

Fundamentally, this principle focuses on the importance of investing in information security only when it is clearly warranted, and in a manner that delivers the optimum treatment for the risk through the lifespan of the investment. It also provides a different context for the business case where, in a bizarre hangover from the desire to invest only in profitable IT projects, investments in information security are also required to demonstrate a positive financial outcome. Rather, a proposed investment in information security should be inalienably linked to clearly identified risk and be demonstrably, the most appropriate option for treatment of the risk.

This does not mean that literally every risk and every individual purchase need be linked through a business case. There is a well-established understanding of the basic elements of information security risk which is matched by well-established, though continuously evolving best-practice in configuring infrastructure and systems to provide the first line of protection. Nonetheless, existence of such knowledge should not be taken as carte blanche for over-spending on technology for the sake of information security – the investment decisions should still carry a clear, if brief, confirmation of risk exposure and fitness for purpose.

Decisions to invest in IT-enabled business systems, whether custom developed or through acquisition of packaged software, should include appropriate consideration of the information security risks for that system and the underpinning technology as an integral part of making the acquisition decision. Given the extent of information security risk faced by a majority of organisations, it should be regarded as unacceptable for consideration of information security to be deferred until after the acquisition is made or construction and integration is complete, as retrofitting information security arrangements is likely to be at least complex and expensive, and may be impractical and unachievable.

This does not mean that the only allowed investments in new capability should be those that incorporate a high level of information security. Rather, it means that the acquisition decision should weigh an unambiguous understanding of information security risk and protection as well as other factors in favour of and against the decision.

Infrastructure decisions today also require specific consideration of information security risk and treatment. The advent of infrastructure and operational outsourcing, software-as-a-service and so-called cloud computing may obviate the need for an organisation to retain skills and provide environments for infrastructure, but they do not absolve the organisation from assuring itself that information security risk at the infrastructure level is properly treated, in the context of its own business activities.

Performance

In ISO 38500, the Performance Principle essentially says that information systems performance should meet the reasonable needs of the organisation – IT should perform well, whenever required.

This should also be the rule for information security. The arrangements for information security should perform well, whenever required.

It might be too easy to consider this point just in terms of the efficacy of the information security arrangements in preventing, detecting and resolving information security incidents. Of course, these matters should be given appropriate and ongoing attention. However, there should also be consideration of how the information security arrangements interact with the complete system of the business, to ensure that there is an adequate balance between the cost of the necessary controls and the efficiency and effectiveness of the business overall. Where there is an unacceptable reduction in business performance or the performance of individuals, there is also often a temptation to circumvent the information security protocols, improving business throughput and performance, but often at significant risk of information security breaches.

The constant nature of some kinds of information security "hacking" means that some of the more basic controls in organisations are effectively under constant test and their effectiveness and performance can be readily measured. However, the more exotic and sophisticated efforts of criminals and other hostile entities are rarely continuous – they are more likely to be sudden, intense and unique. These techniques are also under constant and intensive development, with a significant undercurrent of collaboration by otherwise independent groups enabling rapid development and lightning-fast deployment of new forms of attack. Organisations which assess themselves as being a high probability target for such attacks should use an appropriate ongoing testing regime to give assurance that the information security arrangements are fit for current and foreseeable conditions.

This does not mean however that only organisations with substantial risk should be testing their information security regimes. The reality in today's market is that most organisations have significant risk and thus should all conduct appropriate routine tests.

Conformance

Increasingly, and probably as a consequence of organisations failing to ensure appropriate information security and related behaviour, governments are legislating minimum and sometimes stringent and onerous obligations for information security. With some jurisdictions imposing substantial penalties for confirmed breaches of information security, it is vitally important that organisations are well informed of the relevant laws when considering their information security risk and treatment, and that they remain informed as the legal situation evolves.

Some industries are also acting to direct and control the behaviour of their members, in an effort to ensure adequate information security. In some cases, such as the payment card industry data security standard (PCI DSS) there are significant conformance obligations being imposed on organisations that previously enjoyed almost complete freedom with little, if any recognition of the risk they were taking.

Historically, many organisations approached information security as if the risk lay predominantly with the activity and behaviour of front-line personnel. Internal controls and policies tended to focus on control and use of passwords and restrictions on the use of removable media. While still important, these tools for management of information security risk should nowadays be complemented by a broader range of clearly articulated, well-communicated and enforced policy to govern the full spectrum of decisions and other behaviours involved in information security. It is not the purpose of this paper to deliver an exhaustive treatment of the policies that may be required. However, it is strongly suggested that the principles for governance of IT, and now demonstrated as being also relevant in governance of information security, should form a basis for an overarching set of six policy statements that clearly define the expected behaviour in the organisation's information security risk and treatment, with regard to responsibility, planning, acquisition, performance, conformance and human behaviour.

Human Behaviour

Today's information security risks and challenges are clearly a problem of human behaviour. On the one hand, mainstream human beings are inclined to be trusting and see that in a perfect world, there would be no requirement for information security other than to guard against the possibility of mechanical loss. On the other hand, our communities host individuals and groups who, for a variety of reasons, behave in an unethical manner, seeking to obtain access to, disrupt, damage and otherwise interfere with information held by individuals, organisations and governments.

No assessment of information security risk, and no plans for treatment of such risk can be considered complete unless the relevant aspects of human behaviour are considered and accommodated. In most cases, it is important to identify a variety of human communities on whom the analysis and treatment of risk is focused. These communities often need to be subdivided so that the diverse behaviours can be properly understood.

One of many challenges in contemporary use of information technology is that the people on whom we depend for appropriate behaviour in respect of information security are beyond our immediate control and authority. Where once the enforcement of password security could be enforced by, for example, the consequence of disciplinary action, how does one now enforce password security when most password users are not our employees, but our customers. One can hardly sack a customer, after all.

Effort to properly understand the human communities and their various behaviours is an essential part of establishing an effective information security environment in any organisation. Different communities can and will create quite different exposures in what is otherwise the same business context. Moreover, the response of these different communities to the treatments we may choose could also vary markedly, to the extent that what is a benign demand on one community may be an intolerable imposition on another. One size may not fit all, and important decisions may be required about which subgroup interests are accommodated, and which are denied.

In conclusion

This article has discussed information security from a top level governance perspective. It stresses that information security is indeed an important and ongoing topic for governance oversight. It demonstrates however, that governance oversight depends on management doing a great deal of the leg-work, and provides a context in which governing bodies can direct and control their organisation's arrangements for information security without needing in-depth technology skills. It positions information security as a topic that should be addressed in conjunction with oversight of the use of information technology, as the latter is both the principal repository for, and the primary channel for risk realisation in personal, corporate and government information. However, it emphasises that information security is not merely another duty of the information technology specialists, but is in reality a core duty for every member of an organisation.

Tariq's View

Infonomics has an important new friend. We'll tell you more about him in the next few weeks. For now, it is sufficient to say that Tariq participated vigorously in the last ISO 38500 Foundation Class in Kuala Lumpur, and has moved very strongly to adopt ISO 38500 and the vision it presents of effective, efficient and acceptable use of information technology.

A couple of weeks ago, Tariq read *Gartner's Top Predictions for IT Organizations and Users, 2011 and Beyond: IT's Growing Transparency.* Here he comments on some of its messages.

Gartner says:

> *By 2015, a G20 nation's critical infrastructure will be disrupted and damaged by online sabotage. Depending on the target, one can expect various responses.*
>
> *Governments will pass legislation and launch security-related initiatives, as the U.S. did after Sept. 11. This will boost the sector of the security industry that can provide protection against these attacks, similar to how revamped airport security measures led to the emergence and growth of an industry sector around transportation and airport security.*

Tariq responds:

> In the UAE for example, there is ADSIC (Abu Dhabi Systems & Information Centre). They have turned on the heat on local Abu Dhabi based organizations. We've seen a tremendous increase in organizations achieving the ISO 27000 certifications in this year alone than we've seen in the last 5 years.

Gartner says:

> *By 2015, new revenue generated each year by IT will determine the annual compensation of most new Global 2000 CIOs.*
>
> *Executive and board-level expectations for realizing revenue from those and other IT initiatives will become so common that, in 2015, the amount of new revenue generated from IT initiatives will become the primary factor determining the incentive portion of new Global 2000 CIOs' annual compensation.*

Tariq responds:

> Hence, Corporate Governance of IT! This explains the worldwide growing interest in the ISO38500 Guidance. Top Executives in organizations are feeling the heat. They have obligations towards their shareholders. They are starting to realize that they can no longer leave decisions around IT to IT. They also realize that they can no longer say, nor will it be acceptable to say, that they were not involved in the decisions.

Gartner says:

> *By 2015, information-smart businesses will increase recognized IT spending per head by 60%.*
>
> *Due to the recession, IT investment contribution to business success must now be proven. As IT spending per employee organically increases in these market conditions, enterprise leaders and stakeholders must change their way of thinking that "lower is better" for this metric. Unrecognized enterprise goals will create or promote "value destruction" where the viability of the enterprise will be at risk.*

Tariq responds:

> This has long been a problem. ISO38500 refers to this in the Principles.

Infonomics Education Program

Last month we introduced a comprehensive, integrated package of education to serve the burgeoning global market demand for knowledge about governance of IT and ISO 38500. Now we've finalised the education program for the coming few weeks. It's BUSY!

Two day ISO 38500 Foundation Class

Melbourne (Australia)	April 6/7
Abu Dhabi (UAE)	April 13/14
Muscat (Oman)	April 19/20
Brisbane (Australia)	May 3/4
Sydney (Australia)	May 9/10
Kuala Lumpur (Malaysia)	June 6/7

One day ISO 38500 Immersion Class

San Salvador (El Salvador)	May 24
Buenos Aires (Argentina)	May 27

ISO 38500 Introductory Briefing

Dubai (uae)	April 11*
Abu Dhabi (UAE)	April 12*
Muscat (Oman)	April 17*
Bahrain	April 18*
San Salvador (El Salvador)	May 23
Buenos Aires (Argentina)	May 26

* These events are fully booked.

Foreign Elephants

As announced last month, Waltzing with the Elephant is now available in PDF form through IT Governance Limited.

We're still accepting requests for the first-run print copy of the Spanish Edition of Waltzing with the Elephant.

Beating the Drum

Following last month's Infonomics Letter on getting value from Australia's National Broadband Network, we had the opportunity to emphasise the message in The Rust Report.