The Infonomics *Letter*
Plain Language about Leadership and
(Corporate) Governance of Information Technology

June 2011 Edition

A Dose of Reality

Hello, and welcome to The Infonomics Letter for June 2011. It's the end of the financial year in Australia, and many of us are very focused on ensuring that our financial affairs and tax obligations are in order.

But while financial compliance does indeed stand as a dose of reality, it's far from the only dose of reality that we encounter in this information era. For the owners of some 4,800 web sites, the dose of reality delivered during the past month can hardly be more emphatic. Following numerous examples of information security breaches over the past few months, the risk of information security breach and the risk of cloud computing intersected when hackers destroyed four servers and all associated backups at an Australian company known as Distribute.IT. *In the Blink of an Eye* discusses the governance issues that emerge from this event.

The Distribute.IT case is a clear instance of the risks in cloud computing being realised. We discussed those risks just two months ago in a story we called "Rocks Hiding in Clouds". The story was quoted in the June 2011 edition of Company Director, as part of Domini Stuart's article "Seeing through the clouds". *A Few More Words on Clouds* adds further perspective.

A different form of information security breach was reported during June by the Australian Institute of Company Directors, when a notebook computer was stolen. Comments in the press and in online forums raise some interesting issues. We discuss some of these in *A Testing Embarrassment.*

Several state governments in Australia have tried to establish a Shared Services approach to IT. Most have failed, with South Australia now added to the list, while the new government in New South Wales has announced it will embark on its own shared services journey. We discuss the concept in *Albert Einstein Observed.*

The Information Systems Audit and Control Association (ISACA) has released an exposure draft of its forthcoming COBIT 5 framework. This is a significant work, which has been influenced by the international standard for governance of IT. Some preliminary details are discussed in *COBIT 5 Exposure.*

May and June saw me journey to Argentina, El Salvador and Malaysia to explain the ISO 38500 approach to governance of IT. Fortunately, the travel was all done before ash from the Chilean volcano messed things up. In *Tale of Five Nations*, we compare governance capability in the five nations I have visited so far in 2011.

Mark Toomey 30 June 2011

In the Blink of an Eye

Some time around the middle of June, one or more malicious individuals breached the security controls of an Australian web-hosting provider known as Distribute.IT, gaining access to several servers which were used to run websites owned by Distribute.IT customers. These malicious individuals then ran programs that effectively destroyed the data storage facilities of four servers. For the uninitiated, this can be likened to exploding a bomb in a library, destroying all the library catalogues and shredding most of the books. Given that computers do their work very quickly, it should be no surprise that the damage was caused in a very short amount of time.

What is significant and unusual in this case is that the hackers also destroyed all of the backup copies of the data stored on those servers. To do this, the hackers had to gain access to separate storage devices onto which the customer data should have been copied. As a result, all of the data stored on four machines has probably been permanently and irrevocably lost. According to news reports, this has resulted in 4,800 separate web sites simply disappearing.

Some of those web sites would have belonged to businesses. Almost certainly, some would have been interactive, designed to at least capture information from and about the people who used them. Some may have been live e-commerce sites, processing transactions and taking orders. It is highly likely that all data collected by these websites has been lost.

Just two months ago, in the April 2011 edition of The Infonomics Letter, we discussed the risks of cloud computing in an article titled "Rocks Hiding in Clouds". Companies like Distribute.IT are examples of cloud providers – they provide infrastructure for shared use by other entities on a commercial basis. It is likely that many of the companies that used Distribute.IT facilities would have regarded the company as an arms' length IT department that should "look after all the IT issues". Many would have paid no attention to perceived "technical issues" like backup of data.

Now they have paid the price for failing to understand that users of information technology have significant responsibilities that are separate from those of the suppliers of information technology. The emergence of cloud computing, in all its diverse forms, has brought this into stark relief.

The possibility of a legal remedy would be cold comfort to those businesses that have been severely damaged by the breach of Distribute.IT's security. At best, obtaining compensation will be a tedious affair. In all likelihood, the company won't have any significant realisable assets, partly because the cost of establishing a hosting service is not all that great,

with the probability that most of the equipment would have been subject to finance and partly because the loss of customers and the loss of reputation will have very quickly rendered the business unviable. In actual fact, a commercial transaction has already been completed with another hosting provider taking over the assets of Distribute.IT, leaving the husk in the care of its owners and directors to deal with the aftermath of the hacking event.

As with most cases of loss and damage, the old proverb "an ounce of prevention is worth a pound of cure" is highly applicable. Those who used the Distribute.IT service should have taken steps to ensure that their business was adequately protected against the things that might have been reasonably identified as risk. The six principles in ISO 38500 serve as a framework for discussion.

Responsibility: Just who was responsible for what in the commercial arrangements that existed between Distribute.IT and its customers? Clearly, the company provided infrastructure and it should have provided an adequate security shell around that infrastructure. Perhaps it was required as part of its service to make backup copies of customer data – but what exactly were its obligations in this regard? Was it also responsible for ensuring that backups were retained on media that is physically removed from the network and impossible to access?

Regardless of what responsibility was assigned to Distribute.IT, what responsibility did the owners of affected businesses have for safeguarding their data, and where applicable, the data of others who were using their websites? Would it not have been prudent for them to assume at least a responsibility for ensuring that the data was safe from loss, harm and exposure? Contemporary best practice in information management is strongly oriented to responsibility for the data being first on the shoulders of those who are its owners and custodians, with a lesser responsibility being imposed on those who operate the infrastructure.

Strategy: According to ISO 38500, the plans for IT must serve the needs of the business, while the plans for the business take into account the current and future capabilities of IT. In an arms' length supply context, the plans for Distribute.IT's technology should have met the reasonable needs of its customers, and that should have included an effective and secure approach to backup. However, the businesses that use the Distribute.IT service should also have been aware that most forms of cloud computing are immature, lacking standards, key disciplines and controls. They should have planned for the possibility that Distribute.IT might fail, leaving them with no infrastructure service and no access to their data.

Acquisition: The decision to use an external provider to host a web site is one of acquisition, and carries the expectation that the buyer will make the decision "for valid reasons, on the basis of appropriate and ongoing analysis, with clear and transparent decision making, and with appropriate balance between benefits, opportunities, costs, and risks, in both the short term and the long term (ISO 38500)". No doubt, the choice of an external provider is a completely legitimate choice in many cases today – as long as the purchaser understands that the balance between benefits, opportunities, costs, and risks will be completely different to an in-house supply arrangement. The crucial question that comes from the Distribute.IT case is: "Do the increased flexibility and convenience, combined with the reduced cost, offset the risk of reduced control and the risk of inadequate practices on the part of the supplier"?

How many organisations blindly choose an external supplier purely on the basis of price, with no consideration of the other matters highlighted by the ISO 38500 Acquisition Principle?

Performance: How does a buyer of a commercial product ensure that it performs well, whenever required? In a retail context, we have extensive legal and regulatory frameworks that ensure the quality of products and services. We cannot buy cars that do not comply with strict design rules, because manufacturers are not allowed to sell them. Financial services, telephone and electricity services, health services and many more are strictly controlled. Many contemporary services may only be provided by properly trained and licensed individuals, and many professional occupations carry an obligation to be a continuing member of an appropriate professional body.

When there is an absence of such legal, regulatory and professional control, buyers of products and services take a risk that performance may not measure up to reasonable expectation, and must manage that risk. Until relatively recently, most users of IT managed the risk by directly controlling the infrastructure and environment. They put in place management systems comprising skilled personnel, processes, tools, structure and rules through which they derived reasonable satisfaction that their IT would perform as required. Now, part of the business case for cloud computing seems to be the avoidance of these overheads. The trouble is that removing the need for the buyer to implement these management systems is not necessarily matched by an obligation on the part of the provider to implement corresponding management systems. As we have seen in the case of customers of Distribute.IT, the absence of adequate management systems on both user and supplier sides results in tragic consequences.

There is a clear imperative here. For cloud computing to achieve maturity, it is necessary that an appropriate framework of controls, qualifications and independent assurance be put in place that gives

buyers of services reasonable assurance on the quality, reliability and performance of the product they have purchased.

Conformance: Clear, unambiguous rules are an essential part of everyday life, as are the means of educating people about the rules, and ensuring conformance to the rules. Of course, it is also important that the rules should be necessary and appropriate, and that the sanctions for non-conformance should be appropriate.

As information technology infrastructure approaches the status of ubiquitous commodity, there will need to be rules that apply to that commodity. Such rules and conformance mechanisms will be an integral part of the regime through which buyers of IT services will be assured of quality and performance.

Many of the rules for IT already exist, though they lack an effective regime in which conformance can be reasonable assured. In many cases however, the rules do not exist as a formal and universal mandate. Rather they exist as the internal policies and controls of individual organisations, backed up by an extensive body of formal and informal knowledge. One topic for which many organisations with long-standing IT environments have rules is the protection and preservation of data. The rules for backup and archival retention of data are in many cases underpinned by legal obligations, but are also often left entirely to the IT department, because backup and archival are perceived to be "technical tasks".

Until there is an adequate regime of regulation and oversight for cloud computing, at least on a par with electricity and telecommunications, and preferably with the controls that apply to banking and finance (information should be regarded as, and sometimes IS money), there remains a need for buyers of services to verify that the capabilities, controls and safeguards they require are written into enforceable contracts with right of proactive verification as well as substantial remedies in the case of non-conformance. If this is not possible, the buyers will need to ensure that they put in place their own arrangements to afford the protection they require.

Human Behaviour: There are several aspects of human behaviour that contributed to the loss experienced through the hacking of Distribute.IT. The buyers of the Distribute.IT service were arguably too trusting and complacent – either not knowing how much risk was attached to their purchase, or simply expecting the supplier to completely manage that risk. The operators of the Distribute.IT business may have lacked the interest and motivation to provide effective security, and they may have not thought through the potential risk of leaving backup devices permanently attached to the network. They may have had unreasonably high expectations of their customers skill and understanding. They may have been reluctant to invest in what may have been a marginal business, or they may have been reluctant to spend in the hope of making a killing in an emerging market. They may have held supreme belief in their own skills, unable to recognise the possibility that their hidden opponents might have deeper skills.

But perhaps the biggest human behaviour issue that we should attach to this incident is the one linked to how we deal with the criminal act that has been perpetrated. This incident once again reminds us that not all people are committed to the well-being of others. There are many who have the technical expertise to break into computer networks and damage them, and regrettably many of them lack the moral integrity that directs them away from using their talents in a harmful way.

When people act with malicious intent and destroy or damage or deny access to or otherwise inappropriately deal with valuable property, our legal system provides for those people to be brought to justice and face the consequences of their crimes. However, the information age brings two problems of human behaviour that we must solve as we face the increasing prevalence of crimes against information. The first is the problem of presence. The second is the problem of value.

The problem of presence arises because, unlike most cases of criminal damage to a person or property where the perpetrator needs to be physically present for the crime to occur and there is thus clarity of jurisdiction, in a crime against information, the perpetrator needs only a communications network and can be physically far away – out of physical and legal reach. There needs to be a concerted international effort to develop a framework in which the perpetrators of crime against information can be brought to justice as would be the case for crimes against persons and physical property.

The problem of value comes into focus when we consider the disparity in consequences handed down by some courts for crimes against information compared to those applying to crimes against property. There seems to be a tendency of the learned persons who adjudicate in the courts to regard a crime that damages information as being of lesser impact and consequence than a crime that damages property. We need, with considerable urgency, to develop a new paradigm in which prosecutors and judges fully understand the financial impact that goes with a crime against information.

[top]

A Few More Words on Clouds

Cloud computing is a fact of life, and probably won't go away. The term is so deeply entrenched that it may become one of the few buzz-phrases of the IT industry that never fades. However, cloud computing is still very new, and we have a great deal to learn, not just because of the new technology (actually,

most of the technology for cloud computing has been around for a while), but because of the radical changes it brings to the ownership and control regime. As argued above ("In the Blink of an Eye"), there is a need for considerable development in regulation and oversight before we can be truly comfortable that cloud computing is safe.

Domini Stuart writes for *Company Director*, the official magazine of the Australian Institute of Company Directors. She has done several useful articles on aspects of information technology, and it has been my pleasure to provide input to some of those articles. Her June 2011 article "Seeing through the clouds" is a case in point, where she weaves a very useful discussion through inputs from several expert commentators, consultants and suppliers.

However, there are a couple of points in the article that really warrant further discussion.

According to the article, Aidan Tudehope, co-founder and director of Macquarie Telecom, describes cloud as a way of buying computing and storage in the same way as buying power – saying that "You pay for what you use as you use it".

The article acknowledges that unlike power coming in, cloud is about data going out and the associated risks are far more varied and complex. This risk is emphatically presented in the case of Distribute.IT.

The analogy with electricity can be greatly improved if we look at the whole picture. The electricity industry is heavily regulated with emphasis on continuity and sustainability of supply. However, there is little such regulation in cloud computing and even standards are only now beginning to emerge. Even with regulation, organisations that critically depend on electric power usually put in place backup power supplies. What does one do when the data is "out there in the cloud" and access has been cut off?

Stuart's article also quotes Bruce McCabe, Director of Innovation in KPMG's IT Advisory group, who says that smaller businesses are accepting major service interruptions, behaving as consumers.

That may be true. However, small business does not need to be powerless from the outset, and should not be powerless when isolated incidents become routine failures. As with any other acquisition, small business must exercise care in initial selection of service provider, noting that leverage diminishes greatly once the service is loaded and running, and that the pain of relocating can be greater than the pain of enduring an unreliable service provider. And regardless of the attraction in the deal, small business must remain sufficiently in control that it can, whether through choice or through force majeure, rapidly and effectively relocate to an alternative supplier. This means at a minimum that there must be a clear understanding of the data handled by the cloud provider, and a reasonably current and useable copy of the data that is accessible regardless of the status of the provider.

There is a huge temptation to treat cloud computing as a great saviour that eliminates the cost and pain of owning and operating your own IT. Cloud providers of course want us to believe that, because it is through such belief that they will make their money. However, cloud computing does involve trade-offs, and it is vital that those making decisions about cloud computing do so with strong understanding of the trade-off.

One way to understand the cloud computing paradigm is to consider the difference between owning and driving your own car, and using taxis. Each has its place and for most, a mix of the two is ideal. But whether one uses taxis or self-drive, it is the individual who decides when and where they are going. In every cloud computing scenario, the user of the service must remain in control of its own agenda, and must ensure that the cloud serves its purpose effectively.

In a business choosing to deploy systems using cloud computing, infrastructure and on-demand applications are only part of the story. To gain the maximum value from any investment in IT, it is essential that organisations first establish very clear, measurable objectives and then go ahead to carefully plan and implement the complete picture of business use, including adapting business process, adjusting organisation structure and controls, and gearing up the people who are affected by the change.

Cloud computing, like every technology breakthrough, has potential value when used well, but is far from the Silver Arrow that magically unleashes the business high performance genie with no additional effort.

[top]

A Testing Embarrassment

Another June 2011 incident has caught the interest of a large number of LinkedIn members in two separate discussion forums. This was the theft of a notebook computer from the Australian Institute of Company Directors. Details of the theft were notified to AICD members (including myself) a few days after the incident, and subsequently reported through several press channels.

The requirement to notify members arose because the stolen machine contained a substantial set of member and contact data, some of which many AICD members would regard as private, if not sensitive. We are told that although the data is not encrypted, it is subject to a number of safeguards. We are also told that the theft is regarded as an opportunistic event that occurred during a weekend building power outage that disabled door security, and despite the presence of additional security guards. The message to members and other contacts from the AICD is

written in measured tones that appear designed to minimise concern arising from the event. The text does not deny the risk of the data being used, but does present the risk as being relatively small.

One point that is not explained in the AICD letter to members is the reason why a substantial set of member information was on the notebook in the first place. Normally, one would expect such data to only exist on a server in a properly secured environment, and managed by an appropriate business application. However, one of the press reports states that the data had been loaded onto the notebook for use in testing the AICD's new Customer Relationship Management (CRM) system. Taking this report at face value, a number of subsequent commentators have noted that the use of live data for testing has for a long time been regarded as very poor practice. Some have noted that good practice in stewardship of data includes a formal policy setting out the legitimate use of data, as well as responsibility for its management, integrity and security.

If the report is taken at face value, the question then arises as to whether the AICD has established appropriate policies regarding the use of data. If such a policy exists and is observed, most likely the data would not have been on the stolen laptop and if it had, it would have been subject to strong encryption. However, while there have been many cases across many organisations of policy being ignored leading to similar incidents, there is also the possibility that no policy existed, and that nobody had given any thought to whether or not such policies and associated controls might be needed.

According to the letter from the AICD, action take includes involvement of the police, forensic experts and advice from the Privacy Commissioner. This is a significant response to a single incident and demonstrates that AICD does recognise the sensitivity associated with the data that has been stolen.

Taken as a single incident, in most organisations, the information provided and the action taken by AICD may well be regarded as sufficient. However, at least one commentator has noted that a body principally concerned with governance should demonstrate impeccable governance over all of its own activities, including its use of information technology.

Karen Scott Davie commented on the incident in a LinkedIn discussion. She said: *"As a graduate and member of AICD and as a Chief Information Officer, I was alarmed that the privacy of member data, especially given the calibre of the AICD members was able to be compromised so easily. It (the incident) demonstrates the absolutely critical need for proper IT Governance, Risk Assessment and compliance within any organisation. This is a strategic business issue. It is a risk and responsibility that rests with the board members and one of the reasons company boards must include ICT skills and experience within their board members in order to fully understand the business risk and reputational issues at stake"*.

Considered in the light of the many IT security problems reported during 2011, the AICD incident may prove to be quite minor. However, it might also present a valuable learning opportunity for the AICD, its members and other stakeholders. Although there are factions in the director community that continue to deny the need, there are many pointers to the importance of effective board level oversight of IT. These include increasing regulatory burden relating to information, emergence of specific guidance for directors such as in South Africa's King III Report on Corporate Governance, the persistent problem of damage to organisations through avoidable failure of both IT initiatives and operational IT systems, and the increasing frequency and severity of malicious attack on IT systems and networks. For those directors who are unsure, and for those who are already convinced of the need for them to oversee the use of IT, a great deal of value could be derived from AICD using the incident as a trigger for a comprehensive review of the arrangements it has in place for governance of IT. The learning from such a review should, in addition to improving any identified weakness in the approach used by AICD, also provide a source of knowledge for AICD members.

This review should of course be conducted using the ISO 38500 framework. One wonders how close the AICD might be to the ideal of good governance when measured across the six principles set out in the standard. The result of a formal, structured assessment may surprise!

[top]

Albert Einstein Observed

The definition of stupidity is doing the same thing over and over again and expecting different results. — **Albert Einstein.**

Einstein's point has been demonstrated many times as organisations around the world have attempted to wrestle information technology into submission. One case in point has been the attempts by several state governments in Australia to adopt a "shared services" model for government computing.

Western Australia started its effort in 2003, aiming to standardise services for 90 agencies. Due for completion in 2006 at a cost of $91 million, the project was reported in late 2010 as being likely to continue until 2013, at a cost of $400 million.

Queensland adopted a shared services strategy for IT at around the same time. The strategy effectively crashed with the disastrous May 2010 implementation of a payroll system for Queensland Health, resulting in many staff not being paid the correct amount on time (the most fundamental purpose of a payroll system

should be to pay people the correct amount, on time – see discussion in The Infonomics Letter June 2010).

South Australia embarked on a similar journey in September 2006. A 28 June press report SA Coalition slams shared services "disaster" highlights that all is not well with this initiative, with budget overruns of more than 100% and benefits no longer available.

Meanwhile Victoria took a quite different approach to shared services in 2005, which evolved into the entity known today as CenITex. The Victorian model differs substantially from those in Western Australia, South Australia and Queensland, because the focus of CenITex has been on shared infrastructure, rather than shared business systems. CenITex has avoided most of the complexity that makes business systems change extremely difficult – the human behaviour that is a fundamental part of the change.

Part of the problem seems to be that the term "shared service" does not tell the entire story. The WA, SA and Queensland models actually go beyond shared services, with the value being predicated on substantially standardised business systems – which are possible only when agencies all work the same way. Such standardisation is a characteristic of the approach used by government in Singapore, where the business architecture is the lead element in standardisation, enabling subsequent adoption of standard business systems and infrastructure. A failure to standardise business, as was the case with the payroll projects in Queensland, means that the sharing is limited to a few base elements, such as the name of the supplier of the software.

Now New South Wales, under a new government, is also embarking on a Shared Services journey, with the concept being central to an initiative to develop a new state-wide strategy for IT.

This will be an interesting process to watch. Shared services models are still widely promoted as "best practice" even though they often fail. One wonders whether NSW will aim for the tough grind of standardising business systems across what may be an unwilling state public service, or the more straight forward merging and standardisation of infrastructure.

[top]

COBIT 5 Exposure

ISACA, The Information Systems Audit and Control Association has long been a strong advocate for effective governance of information technology. Through its IT Governance Institute, ISACA has championed the concept of board responsibility for, and engagement in governance of IT. However, the practice guidance on ISACA frameworks, and particularly in COBIT (currently at version 4.1) has been heavily focused on management activities, and has lacked a clear conceptual separation of governance and management. This lack of conceptual separation has also impacted one of the flagship ISACA qualifications. The knowledge specification for CGEIT (Certified in the Enterprise Governance of IT) is dominated by management skills, and requires little real governance expertise.

ISACA signalled that this would change during 2010 when it released the first exposure draft for a major overhaul of COBIT. The draft bluntly acknowledged the lack of conceptual separation, and foreshadowed a major shift in thinking, underpinned by the concepts in ISO 38500.

Just a few days ago, ISACA announced that a draft of the new edition, COBIT 5, is available for review and comment. The COBIT 5 Exposure Draft material is freely available and the comment period remains open until 31 July 2011. The draft comprises two documents – an 85 page framework and a 218 page Process Reference Guide.

A brief scan of the framework reveals a definite influence from ISO 38500, with explicit acknowledgment of the standard and the three principal tasks of governance – Evaluate, Direct and Monitor. However the principles for good governance set out in ISO 38500 are not immediately evident. One wonders if they will be revealed through a closer inspection.

I will certainly be allocating some time to the COBIT 5 drafts, and will include a summary of my comments in the July 2011 edition of The Infonomics Letter.

[top]

Tale of Five Nations

In the Infonomics Letter for April 2011, I reported on assessment of how IT is governed in the United Arab Emirates and Oman, following a fortnight visiting those countries. The end of May and early June brought the tally of nations covered in 2011 to five, with visits to Argentina and El Salvador, followed by a second visit to Kuala Lumpur.

The Argentine visit was organised by my good friend Carlos Francavilla and his colleagues at BIT Company, and sponsored by the National Institute of Public Administration (INAP). Undersecretary of Technology Management, Eduardo Thill arranged a major briefing on the ISO 38500 approach to governance of IT for more than 70 government business and IT leaders.

During the briefing, which was conducted in the very grand auditorium of the Cabinet Secretariat, Eduardo Thill emphasising the role of standards for governance of IT in recognising that with the advent of ubiquitous high speed broadband, the user of information technology is a new dominant player, not just in information technology but in every aspect of society.

In addition to the government briefing, a short briefing was provided for leading CIOs in the city of Buenos Aires, and an ISO 38500 Immersion class was completed by 18 leading CIOs and consultants.

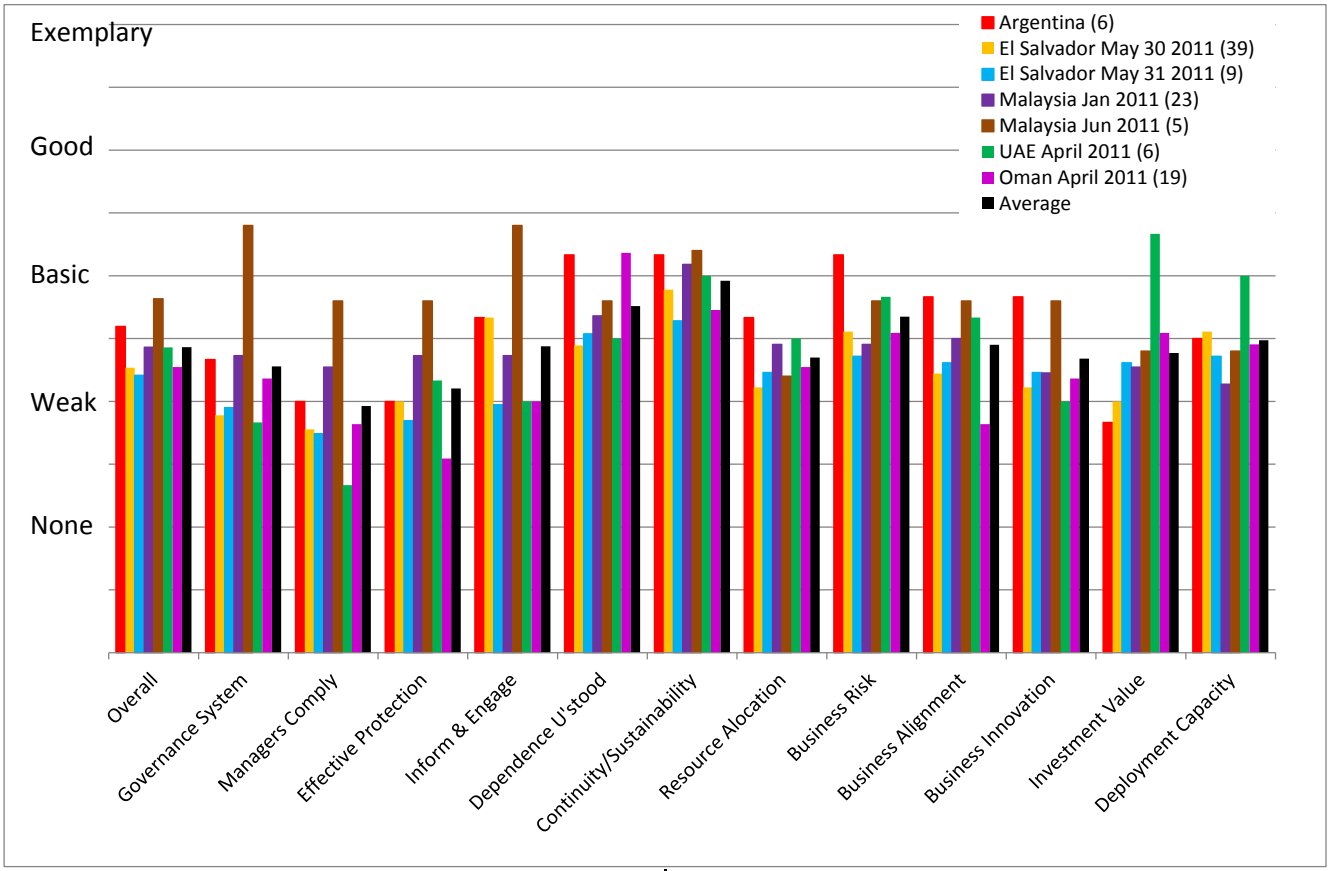
El Salvador may not come immediately to mind when we think of nations that are leading in the IT industry. Thus it may surprise many to know that El Salvador, through the efforts of its fledgling Chamber of Commerce for the IT Industry (CasaTIC) and with the support of the team at BIT Company, delivered 60 delegates to a half day briefing on governance of IT, and a further 45 delegates to a full day ISO 38500 Immersion class.

While the casual visitor may well still see El Salvador as an impoverished nation, there is also a palpable energy and enthusiasm, with information technology being seen as a significant field of opportunity. The enthusiasm and engagement in both sessions was strongly evident, and is reflected in this comprehensive blog post from Lito Ibarra.

Malaysia was one of the first nations to begin embracing ISO 38500 as part of the learning agenda for its business and IT leaders. Since April 2009, I have worked with Expitris Worldwide to run five ISO 38500 Foundation classes, with more than 60 people trained to date.

While the Arab states clearly enjoy the benefits of substantial oil wealth, they are otherwise very much developing economies – building capability for a sustainable future beyond oil. El Salvador, Malaysia and Argentina are also nations that are focused on developing their economic futures. It is rather interesting and pleasing to see that these developing economies are looking more and more to embracing the guidance in ISO 38500, to improve the likelihood that their investments in IT will deliver valuable outcomes.

However, merely attending briefings and classes on governance of IT is only the start for these nations. Performance comes not from learning about possibilities, but from making real change to improve performance. As always, assessments were conducted in all of the classes across the five nations as part of the Immersion and Foundation classes. These assessments show that established practice has delivered the developing nations around the same level of capability in governance of IT as is typically observed in the "developed world".



The chart presents the combined "indicators" assessment results from seven separate classes run in five nations during 2011. The numbers at the right in the legend are the sample size, which ranges from 39 in El Salvador on May 30, to 5 in Malaysia in early June. The "indicators" are 12 points of performance and capability that can be used to form an approximate initial view of how well any organisation governs its use of IT. In a full assessment, the indicators are complemented by a further 72 points linked to the principles defined in ISO 38500.

In the assessment, class participants are asked to compare their organisations' approach, capability and performance to a set of exemplar statements. The

ranking express how closely organisations conform to the guidance and expectations of ISO 38500, and how well they govern their use of IT. The profile for each group is the average of all responses, and gives an initial perspective on the overall effectiveness of governance arrangements in the region to which the group belongs.

It is rare for a participant to claim "exemplar" status on any specific point of assessment. Most people who undertake the assessment are in fact quite brutal in their self-assessment – and many comment that while the exemplar statements are quite reasonable, there is significant opportunity for improvement. When used in a single organisation, the assessment tool provides a way of rapidly segregating consistent and inconsistent views, and of establishing agreement on both need and opportunity for improved governance of the use of IT.

In the Malaysia June class, one individual consistently claimed exemplar status, driving up the class average. Other responses were more consistent with the responses from the much larger class in January.

Reading the chart from left to right, we see that the five nations, across seven surveys, **overall** have weak to basic governance of IT. The weakness begins with a tendency to not having a clearly defined **governance system**, and the limited extent to which all **managers comply** with the specification of the system. Without an effective governance system, it should be unsurprising that there is little **effective protection** against things going wrong with IT. While some managers may be well aware of what is happening with IT, it is likely that an effective system for governance would better **inform and engage** those managers, executives and members of the governing body who should be ensuring that IT use is effective, efficient and acceptable.

The pervasiveness of IT and the consequences of IT going wrong contribute generally to a higher level of awareness of the role that IT plays. However, there remains a significant gap between the current and desirable extent to which business **dependence on IT is understood.** Efforts by IT supply teams tend to underpin some confidence in the extent to which IT use protects the **continuity and sustainability** of the business, but across the board there remains significant opportunity for improvement. The gap is perhaps exemplified by the fact that **resource allocation** does not meet the needs of the organisations represented in the survey, and the perception that the **business risk** of serious IT failure is not well understood.

Business alignment is a perennial problem, frequently discussed in many forums. The poor ranking across these seven surveys is perhaps explained by the corresponding low ranking for the governance system, management compliance and the extent to which the appropriate people are informed and engaged. A similar point may be made with regard to **business innovation**, where advanced use of IT in support of business innovation depends on a well informed and engaged management team that can properly understand and effectively manage business risk.

Investment value is delivered when IT initiatives produce business outcomes and defined, measurable benefits. Delivering business outcomes depends on a properly engaged and informed management team, which understands that the value of investment in IT comes from attention to the full spectrum of business change, and not just to the IT components. Such attention depends heavily on adequate resource allocation, a sound understanding of how to ensure alignment of IT and business activity, and an effective approach to understanding and controlling risk. The expressed weakness in these areas may also explain the extent of opportunity for improved **deployment capability**, through which IT enabled change becomes an operational aspect of the business for which it was developed.

The challenge in each of these nations, as is also the case in the "developed world" is to understand more deeply the factors that lead to the widespread weakness in governance of IT, and to develop the capabilities and behaviours necessary to replace this weakness with effective robust capability that ensures an ongoing effective balance between cost, risk, opportunity and value.

[top]

Infonomics Education Program

After a quite intense three months of travel, we are taking a short break from the Infonomics education program in July.

In September, I will be in London for a meeting of the ISO/IEC working group that manages ISO 38500. I'm now working with business partners across Europe to plan events that will enable many more business and IT professionals to become familiar with the standard and the concepts it presents for effective governance of IT.

Suggestions and requests for education events are always welcome – send them to mail@infonomics.com.au.