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

April 2011 Edition

Daring to Dream

Welcome to the bumper April 2011 Infonomics Letter.

At Infonomics, we dream of a worldwide boost in well-being and wealth, driven by a sustained improvement in innovative and highly successful use of information technology, underpinned by business leadership and effective governance.

This dream is central to the Infonomics mission of improving the effectiveness, efficiency and acceptability of IT use by organisations worldwide, through improving their governance of IT.

During April, it was my privilege to share this dream in the United Arab Emirates and Oman, as a guest of EXCEED IT Services and Training. We spoke about ISO 38500 and improving governance of IT to substantial audiences in three cities, and conducted two ISO 38500 Foundation Classes through which we can share some insight into the calibre of the region's governance of IT. See **Middle East Developments**.

It can be very hard to make serious time to read serious books. The trip to the Middle East gave me an opportunity to get started on **Geekonomics** and gain new insight into some of the reasons we have so much trouble with Information Technology.

Last month's discussion on governing information security generated significant feedback and some additional activity that will develop during coming months. Meanwhile, security incidents keep emerging. See **More on Information Security**.

As if security breaches are not enough, April also saw some of the risk in Cloud Computing being made crystal-clear. Cloud computing may be exciting development, but the cloud is not without risk, as discussed in **Rocks Hiding in Clouds**.

Although it is titled "Governance of Information Technology", ISO 38500 makes it plain that its focus is on the use of IT, and that the success of organisations using IT is dependent on the way they go about integrating it into their strategy, their execution of strategy and their operational management. For several years, Infonomics has been at the forefront of argument that IT cannot be treated as an independent issue, and that its governance must be an integral part of governing the ongoing development and operations of the organisation, with business leaders taking responsibility and being accountable for the effective use of IT in developing business strategy, building business capability, and running the ongoing business. In **Gartner's Eureka Moment** we discuss how the well-known IT research and advisory company has also discovered this message.

Mark Toomey 30 April 2011.

Middle East Developments

For many of us, the Middle East, and particularly the six nations that make up the Gulf Cooperation Council (GCC) are synonymous with oil. There can be no doubt that these nations have been fortunate to derive great wealth from the combination of their oil assets and the unquenchable thirst the developed world has for that oil. But in time – the oil will run out. While the developed world must plan for this and develop alternative sources of energy, so too must the Gulf States plan for it and develop new sources of wealth!

Already, the United Arab Emirates cities of Abu Dhabi and Dubai, and the Oman capital, Muscat, have developed far beyond the stereotypical garish displays of unbridled wealth. They are cities breaking through to diversified economies and business centres, in which modern business practices, skills and technologies are now deeply integrated with the culture of the diverse peoples that make up their population. They are also cities that have experienced the impact the recent economic downturn, in their individual ways, are now moving again to advance economic growth.

Building the nations and economies of the future for the GCC means that both government and business in the region are increasingly dependent on information and communication technology. Both the UAE and Oman have dedicated government agencies to provide leadership in this field, and both nations have thriving IT services industries.

For more than ten years, as part of the region's ongoing economic development, EXCEED IT Services and Training has been growing strongly in the GCC region, providing its customers with technology, training and services focused on the supply of information technology. Recently, EXCEED expanded its scope of activity to help organisations make better use of IT as an integral part of business development, growth and performance, bringing new focus to the demand and use aspects of IT. EXCEED's Director of Consulting, Tariq Elsadik, identified ISO 38500 as a key tool for organisations seeking to make effective, efficient and acceptable use of information technology. EXCEED is now building a practice to help GCC organisations become highly effective in their governance and use of IT through adopting and adapting to ISO 38500. Infonomics is assisting EXCEED in this effort by providing intellectual property, tools and techniques developed and proven in the Australian market, along with practical on-the-ground assistance in initial marketing and engagement delivery.

During April, to introduce its new service concepts and to launch the concepts embodied in ISO 38500,

EXCEED conducted a series of launch events – one each in Dubai and Abu Dhabi, and two in Muscat. At each of these events, which were attended by substantial numbers of IT leaders and a few business leaders from government and private sectors, it was my task to deliver the primary address, to position ISO 38500 and the key concepts for governance of IT in the 21st century.

The relative shortage of business leaders, reinforced by comments from senior IT people both prior to and during the briefings, indicates that the GCC is experiencing similar issues to those evident in other nations – where business leaders are not consistently engaging in the essential business leadership, business change and operational management activities for planning, building and running an IT-enabled business. These observations are reinforced by the observations of Tariq Elsadik (see Tariq's View below) and by results of ISO 38500 Alignment Assessments conducted during the tour.

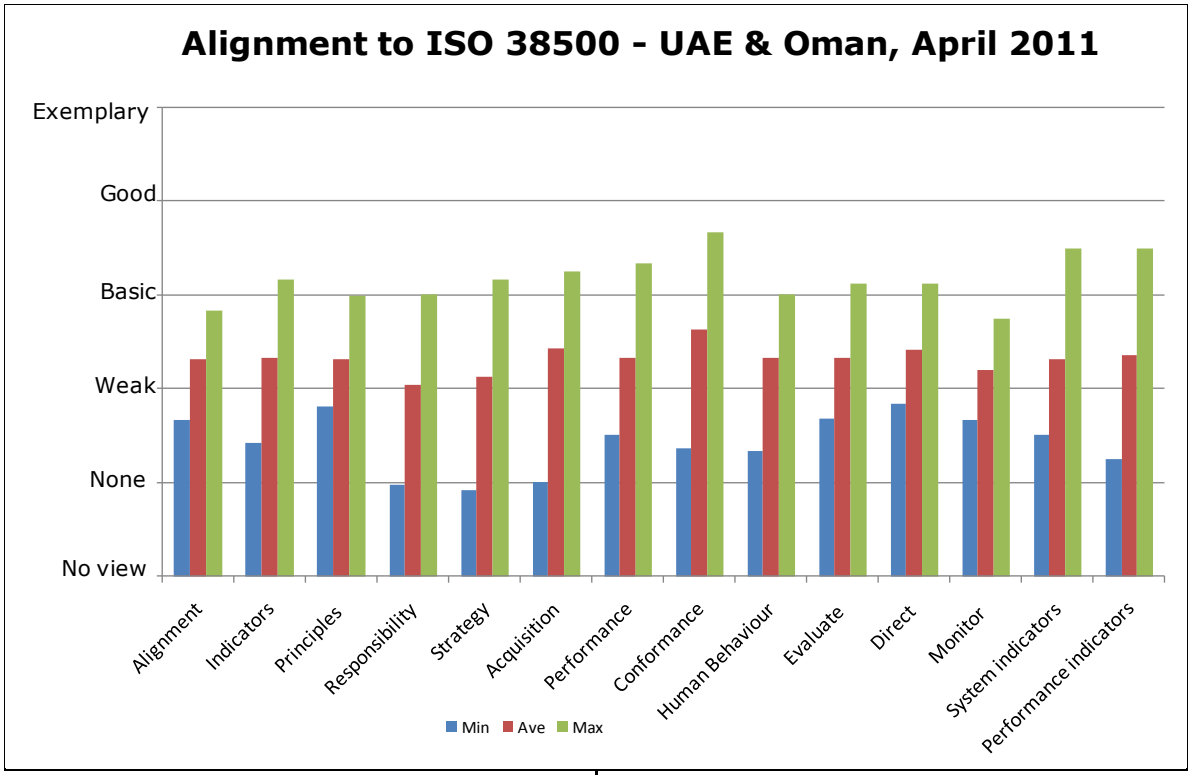
Clearly, there is a context in which it is relevant to introduce ISO 38500 to the GCC region.

In addition to the launch events, EXCEED also arranged two ISO 38500 Foundation classes – one in Muscat and one in Abu Dhabi. These also enjoyed strong attendance, with CIOs and other top level IT managers making up the majority of the class in each location. The thirst for knowledge and insight meant that these were the most interactive classes I have delivered since the two day class was first delivered in Germany, in 2009.

A key component of the ISO 38500 Foundation Class is the self-assessment. Each participant scores his or her selected organisation's effectiveness in governance and use of IT using an 84 point diagnostic comprising twelve broad initial assessment points known as the "Indicators", and twelve assessment points for each principle. For each principle, there are three groups of four points, corresponding to the basic governance tasks of evaluating, directing and monitoring (the current and future use of IT), as defined in the model for governance presented in ISO 38500.

Almost universally, in every nation where it has been used, the diagnostic reveals that governance and performance of IT use are in need of significant improvement, and this was also the case for these two classes. The following chart presents an overview of the combined assessment scores given by participants in the two classes.

The chart presents the assessment results as the lowest, average and highest scores across the sample group. The first set of three columns depicts the overall "index of alignment", or effectiveness of current arrangements for governance of IT, which is the composite view derived across the entire 84 point diagnostic. Subsequent column sets present various subsets of the data.



Interpreting the charts requires an understanding of the scale used to rate the effectiveness of the prevailing arrangements for governance of IT. A technique for this that has proven effective with many audiences is to contrast the assessment of how well an organisation governs its use of IT with an assessment of how well an individual drives a motor car. Thus, "No view" for a person driving a car means not just that they can't drive: they don't understand what a car is for. An organisation at this level with governance of IT would lack organisational awareness of the role IT plays in business.

To score "None" on the driving scale, a person would know what a car is, but have no idea of how to operate the car. For governing IT, "None" means being somewhat aware of the role of IT, but having no concept of how to govern its use.

At the "Weak" level, an individual should be able to get into a car, start its engine and make it move forward. However, at the first obstacle, or very soon after, a crash would occur. Organisations with weak governance of IT can identify some use for IT, and may be able to launch some IT related initiatives. However, most initiatives will fail early, even if the failure is not recognised until considerably later.

People with "Basic" driving skills appear quite competent on the surface. They can use a car confidently to perform routine tasks and journeys, including shopping trips and holidays. However, when confronted with dangerous circumstances, such as an unrestrained animal on the road, severe weather or another driver losing control, they are highly likely to experience a crash in their own right. Companies with basic governance of IT can formulate some plans for the use of IT, launch some initiatives, and conduct normal IT-enabled business operations. However, when something goes wrong, these organisations are poorly equipped for early recognition of the problem and have very limited ability to take effective corrective action.

"Good" drivers have well-developed skills that help them plan ahead to avoid danger, to act early and decisively to stay safe when an unexpected risk emerges, and can execute emergency manoeuvres to protect themselves and others when the risks turn into real problems. Similarly, organisations that have good governance of IT not only make very good plans for the use of IT, they can execute these plans with a high degree of competence, can make adjustments to maximise value, take appropriate action to head of project failures and are rarely, if ever disrupted by operational breakdowns.

"Exemplary" drivers have invested heavily to master the craft of driving, and have talents far beyond those required for safe and successful driving on public roads. These are the motor racing world champions and their top flight competitors. Very few are truly at the full exemplary level, and many who fall between the good and exemplary levels will struggle mightily, but never attain the pinnacle. One might wonder if any organisation needs to be exemplary across the board in governance of IT – the cost would likely be prohibitive for the vast majority. However, exemplary capability in selected aspects of governing and using IT may be viewed as giving rise to a competitive advantage. Such determination would have to be made on a case by case basis, by the leadership of the organisation in question.

Looking at the chart above, we can see that the ISO 38500 Foundation Class participants overall ranked their organisations as having just a little better than weak governance of IT. The highest scoring individual assessed his or her organisation as having slightly less than basic capability to govern the use of IT. There is certainly a strong indication of room for improvement.

Moving to the right in the chart, we see that the scores for the twelve indicators, and overall on the six principles (72 points in total) are broadly in line with the overall assessment. This reinforces that the indicators are a useful and highly accessible guide to the overall effectiveness of governance arrangements.

Across the six principles, marked differences emerge.

We see weak capability with regard to assigning responsibility and further weakness in formulation of strategy and plans. These however are essential capabilities – organisations which have not clearly and appropriately assigned responsibility to individuals who have the means of discharging that responsibility are likely to have the wrong people making decisions about IT, and basing those decisions on wrong criteria. Those with inadequate strategy and planning oversight are unlikely to work on the most appropriate initiatives, and may not have the capabilities in place to achieve their desired goals.

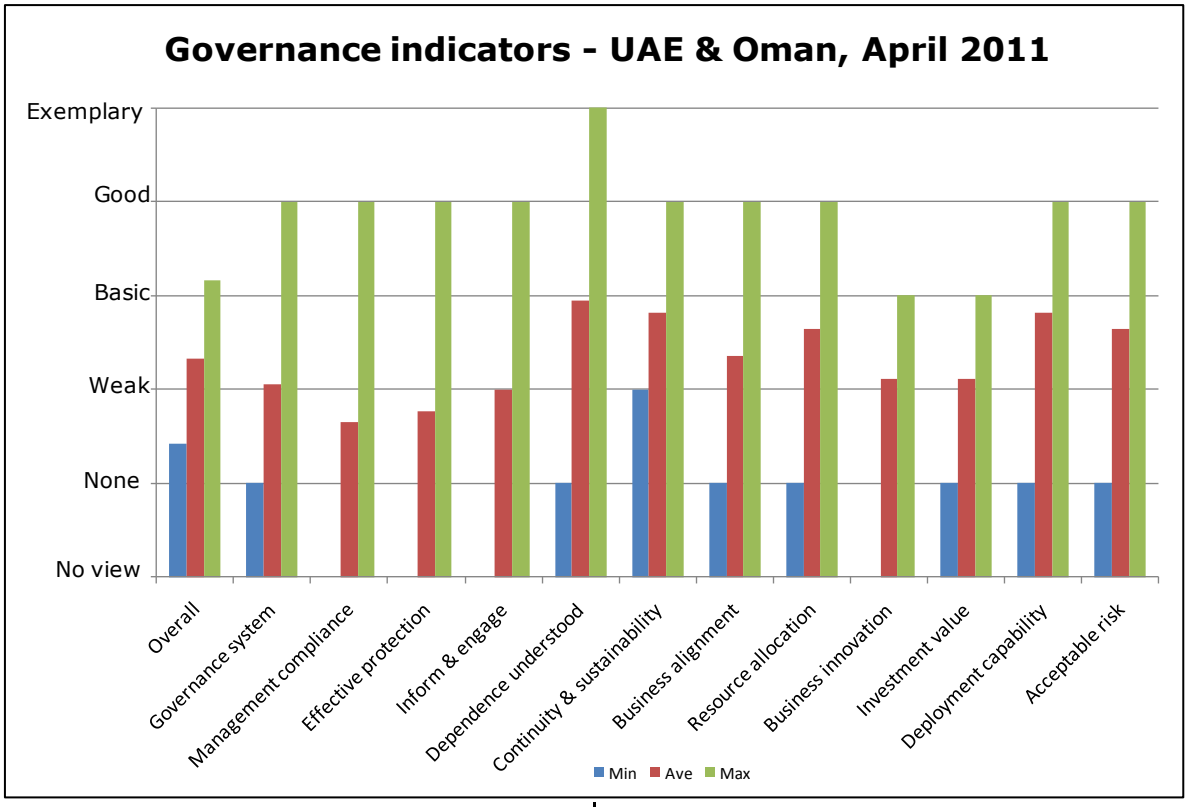
While not yet at the desirable "good" level, the GCC profile is for more effective governance against the Acquisition and Conformance principles, with some relative strength also in the area of Performance. These "bumps" are common across most jurisdictions, principally because in the case of acquisition, established financial, purchasing, contract and similar controls are well-established and mostly benefit from experience with disciplines other than IT. However, these controls do not typically have the sophistication or focus necessary to provide an effective level of governance in respect of IT. Some of the relative strength in performance and conformance also comes often from ability of those involved in the supply of IT to instigate controls that, while often not properly understood by those who use the IT, still have some effectiveness.

On the subject of Human Behaviour, the GCC results are somewhat better than often seen in the rest of the world, with a score well above those for *Responsibility* and *Strategy*. This suggests that arrangements for governance of IT in the region may give a little more attention to the characteristics of people in the process than in some other regions. Attention to human behaviour is critical with contemporary use of IT, because people as individuals and in groups are significant influencers of success with IT, in diverse roles ranging from remote customer to internal employee, business planner and manager, IT specialist and people actually working to deliver project outcomes.

The next three columns – "Evaluate", "Direct" and "Monitor" take an alternative slice through the data,

looking at whether there is balanced emphasis on the three basic tasks for governing the use of IT. The differences in these three items indicate that organisation in the GCC should elevate attention to all three aspects, with monitoring requiring the most improvement. The current data indicates that there is a tendency for some direction to be given but with little analysis and even less follow-up checking. This could result in what direction is given being incorrect or inappropriate, and then not followed anyway.

The final two column sets in the chart segment the twelve "Indicators" into one set that reflect the performance of organisations in their use of IT and the arrangements for governance of IT. The consistency between the two is suggestive of a view that improved governance may improve performance.



A closer view of the Indicators presented in the above chart allows us to explore some correlations and contradictions that frequently emerge. In detailed assessments, these correlations and contradictions are more fully understood through analysis of responses on the principles, face to face interviews and examination of actual documents. The four indicators of performance are those labelled *Business Alignment*, *Business Innovation*, *Investment Value* and *Deployment Capability*. Notice how two of these (*Business Innovation and Investment Value)* are quite low. This suggests that, while IT initiatives are being deployed, they are not creating significant measurable value and not advancing the capability of the business. This is consistent with the low score on *Business Alignment*. Considering the technical supply side dominance of the groups participating in this assessment, the relatively high *Deployment Capability* shown may be more focused on the technical deployment, with less emphasis on the business deployment that is required to release the actual value of an initiative.

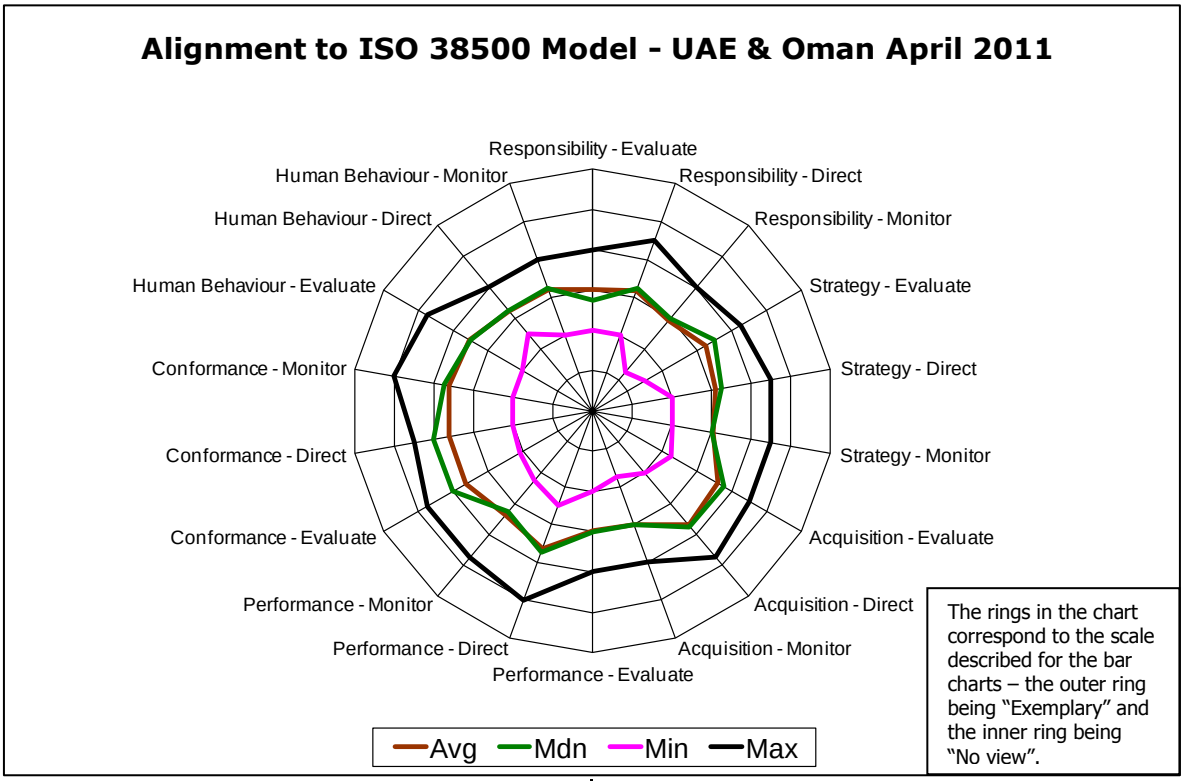
Having even rudimentary systems for governance of IT should help organisations set direction for, derive value from and control risk associated with IT – but only when the system is actually used. The gap between *Governance System* and *Management Compliance* is significant. The absence of a blue bar on the latter suggests that the concept of management following a defined system is a foreign concept in at least some organisations. Weak governance systems and governance systems that are not used will not provide *Effective Protection* against failures, and will certainly not do anything to inform and engage business leaders.

Much higher scores (relatively speaking – they need to be still higher) on *Dependence Understood* and *Continuity & Sustainability* are likely to be a product of the audience that was completing the assessment – mostly senior IT professionals. They would be expected to have this awareness themselves, and some may attribute a higher level of awareness to their business counterparts than is the reality. When used inside a single organisation, the assessment tool frequently shows up stark contrasts in this area.

It is common, yet always disturbing, to note the relatively high score on Acceptable Risk, given the very low scores relating to use of a defined governance system and the leadership being informed and engaged. The low scores on *Business Alignment*, *Business Innovation* and *Investment Value* also

contradict the relatively higher score for *Acceptable Risk*. Again, this may be explained by a predominantly technical audience looking at risk from the supply side, rather than the broader view.

Looking more broadly across the indicators, it is interesting to note that while at least one person graded ten of the twelve points at "good" or better, none graded *Business Innovation* and *Investment Value* better than "basic". This reinforces that even those with perceived strengths probably have weakness that needs to be resolved.



One final chart extends our insight to the calibre of governance arrangements profiled by the ISO 38500 Foundation Class participants. The spider chart above provides a more detailed view on the principles, enabling us to understand the relative emphasis given to evaluating, directing and monitoring in respect of each. There are again some significant anomalies, which help to highlight where attention might be given to improving the governance arrangements, and thereby the overall performance in the use of IT.

Start with *Responsibility*: Within the uniformly low (and therefore unsatisfactory) scores, notice how some organisations pay less attention to working out who should be responsible than they do to actually assigning responsibility, and then few actually monitor to ensure that responsibility is discharged appropriately.

Look at *Strategy*: Organisations seem to put some (more is needed) effort into evaluating strategy and planning issues, but then do not follow through to put the plans into action and check that they are realised.

Now focus on *Acquisition*: Higher levels of control here in evaluating options and directing acquisitions are undone by a lack of monitoring.

For *Performance*, the minimalist approach to evaluation makes one wonder about the origins and legitimacy of the direction given, and the limited monitoring might cause us to wonder if performance gaps are at all well understood.

Conformance often scores high, as previously discussed, but again the pattern is one where monitoring falls away, leaving one to wonder if organisations are at risk of conformance breaches despite having put some rules in place. It is also evident here that a small number of respondents scored higher on evaluating and directing conformance than the main body, and that the majority scores these points much closer to weak than to basic.

Finally on *Human Behaviour*, one relatively high scorer does not offset the overall picture that most of the organisations pay uniformly little attention to the characteristics of people in the process.

The snapshot provided in this assessment is limited by the supply side bias in the sample audience. Notwithstanding it does strongly suggest that there is need and opportunity for substantial improvement in governance of IT in the GCC region, and the number of senior IT people involved gives confidence that there can be strong push for improvement in this space. It may be necessary for the push to begin in the supply side, but by increasing the focus on business issues and related governance matters, a progressively deeper engagement of business leaders should be expected and encouraged. [top]

Tariq's View

I have long been fascinated with the so called divide between IT and Business. As a former CIO for one of the largest company groups in the UAE, I had the privilege to work with very talented individuals both within the group and, whenever I had the chance to participate in CIO roundtable discussions, with other CIO's in the region. Reflecting back on that experience, one thing is for sure, it seems that the issues that we were discussing back then still puzzle us today. Indeed, we are still talking about IT Business alignment if there is ever such a thing, Service and Security Management, skill shortages, staff turnover etc. This view is reinforced by the data that I had collected prior to launching Exceed's Enterprise Governance Management Practice (EGMP).

I spent almost two weeks interviewing CIOs and other IT leaders in the public and private sectors asking the one million dollar question; what keeps you awake at night? The answers clearly point to one observation, that despite the advances made and the experience gained from using the various IT best practices tools that we see around, IT leaders have not been able to crack the code, not just yet. Why is that? I certainly have my views on the matter. For years, IT leaders have been consumed by the supply side of the equation. IT has certainly made advances on that side. But as Mark points out, this is 'polishing the kettle from the inside'. What about the demand side (the outside)? Who is responsible to crack that code? What tools do we have before us today that will allows us to dwell into this subject and make some advances like we've done from the inside?.

I hold the view that as IT leaders, we have the responsibility to learn and master the business vocabulary. We need to recognize that our business counterparts recognize today more than ever, that IT is indispensible to their business, that the business side is ready to engage in business talk about how IT can enable business transformation and change. The sooner we recognize this, the sooner we can unleash the potential of IT.

Go into any organization today, public or private and ask one question: Who makes decisions about and manages the portfolio of IT investments? If the answer is 'the business' then that organization is probably well on its way to cracking the code; but if the answer is 'IT makes those decision' then "Houston, we have a problem"! [top]

Geekonomics

David Rice is an expert on information security expert. He's also an entertaining and insightful author. His book, *Geekonomics: The real cost of insecure software* (ISBN 0-321-47789-8) provides a compelling insight into why we have so much trouble with information technology, and why it will likely get worse before it gets better. Rice draws on analogies to describe the role of software and the behaviour of software "manufacturers". He likens our contemporary dependence on software to the construction industry's dependence on cement. (Portland Cement enabled a building revolution and cement-enabled infrastructure has become ubiquitous in construction: software enabled a business revolution and software based infrastructure has become ubiquitous in most economies). He also likens builders of software to the automotive industry of the 1950's and early 1960's – where form was far more important than function, and where buyers were both willing to take the risk of unsafe product in order to acquire the latest fashion, and individually unable to exert the pressure required for change that would result in safer vehicles.

Rice's discussion draws heavily on we'll-established economic theory, mass psychology and market dynamics. With respect to our propensity to accept defective software, Rice proposes that the market model which has emerged would drive out of business any software manufacturer that sought to differentiate by producing truly defect free software because the cost and time required would drive away the customers. The market is self-defeating and, like the automotive industry of fifty years ago, Rice suggests that only strong government intervention will drive the fundamental change required to bring us a higher standard of software.

Exploring the contemporary problems of today – hacking, electronic espionage and identity theft, Rice draws parallels with the "Broken Windows (the glass ones) Theory". Broken Windows explains why unkempt neighbourhoods quickly become completely derelict. Rice suggests that bad software is an irresistible magnet to those who would exploit it. He notes that even the current extraordinary cost of cybercrime, which he puts at 1% of GDP for the United States, does not seem sufficient to trigger a response. He also points out that (in 2007) the US estimate of 5% of cyber-criminals being prosecuted may be based on a significant under-estimation of the actual extent of cyber-crime. Sadly, he also notes that penalties for cyber-crime are pathetically low when compared to similar crimes committed in person. To complete the scene of despair, Rice points out that many cyber-criminals operate beyond the reach of the jurisdictions in which their victims live, and in at least some cases, these criminals may be state-sponsored. [top]

For me, Rice's book is deeply confirming what I have known for a long time – that our aggressive pursuit of advantage through software has a potentially deep cost, and that we are getting closer to an inflection point where we realise that something must be done. By the time I write the next edition of The Infonomics Letter, I will have finished the book and will certainly write more in summary and response to Rice's propositions.

But for now, let us just consider how apposite Geekonomics might be in the context of the following pieces – *More on Information Security* and *Rocks Hiding in Clouds*. [top]

More on Information Security

Last month's Infonomics Letter focused on governance of information security. It immediately went to the number one spot in terms of reader feedback and commentary – clearly information security is a matter of significant concern for many, and guidance on top level oversight of information security is keenly sought. Reading Geekonomics could hardly have been a more timely exercise.

One comment from Germany noted that I had not mentioned ISO 27001. This international standard defines requirements for an auditable information security management system, and is part of the broader ISO 27000 family of standards on information security. As they stand, the ISO 27000 family provides a comprehensive set of guidance on the management systems required to look after information security.

There are some who would argue that management systems such as those for information security should include a governance component. However, this is impractical, as to follow this logic would require the governing body to be acting across too many diverse "governance systems" with inconvenient and inappropriate segregation of the subject matter. It would also draw the governing body too deep into the detail. What is far more important is that governing bodies have broad guidance in a small set of consistent frameworks, and the purpose of the article last month was to demonstrate that the topic of information security can be addressed most effectively through application of ISO 38500.

While ISO 38500 does provide a suitable umbrella for governance of information security, and the ISO 27000 family does provide extensive guidance on the detail, my ongoing pondering of the distinction between governance and management is leading me to the view that there may be space for an intermediate level of guidance in several aspects of information use within organisations – including information security. This intermediate level of guidance would focus on the role and engagement of executive managers as they collate the proposals for evaluation by the governing body, enact the governing body's direction, and gather the information required to enable the governing body's ongoing monitoring and oversight. I wonder if anybody has any significant thoughts on this.

Meanwhile April is going to go down as one of the significant months for data leaks and theft. If ever anybody doubted that the world is now beset by serious problems of crime related to unauthorised access to and use of personal and organisation information, the hacking of the Sony PlayStation Network exposing details of millions of users, another hacker gaining access to the customer files of German software company Ashampoo (who by the way are developers of information security solutions), and at the beginning of the month, the massive breach at Epsilon, a provider of mailing list services used by many companies around the world.

Thinking about the deepening and seemingly pervasive and perhaps unstoppable problem of providing information security, one has to wonder if we are actually tackling the problem the right way. Very obviously, the information systems that we have today are inherently extremely insecure, and we seem to be going to extraordinary lengths to enclose these insecure systems in impenetrable shells that are proving themselves over and over again to be rather less impenetrable than we need. At the same time we seem to be putting more and more information in environments where it is at higher risk to unauthorised access than ever before. Is there another way to address this problem?

Intuitively the answer is obvious: rather than putting shells around our intrinsically insecure systems, should we not make our insecure systems secure in their own right? However, while this is an easy proposition to make, it is far more difficult to put into action – the costs would be enormous. Probably the tipping point will come when we finally realise that the cost of inaction, or the sum cost of the inappropriate and inadequate defences we use today, combined with the cost of the crimes that do get through those inappropriate and inadequate defences becomes such that we collectively say "Enough".

The change will not come easily. If it were only about writing better software and designing better systems, it would be hard enough – that would require investing to develop higher and more robust skills and qualifications for people who design and build IT systems, and more time and money to enable the more robust designs to be properly built and tested. But change in information security is not just about the software and systems design – its also about the behaviour of people – that so often overlooked sixth principle in ISO 38500. Consider three illustrations – the TomTom Furore, the iPhone Tracker and the Email from an Airline.

The **TomTom Furore** emerged in the Netherlands during the past few days. TomTom make navigation systems for cars and the more recent models have a the means of making two-way connection back to the TomTom HQ. They can easily download the latest maps – giving drivers the best possible chance of taking the best route. They can also upload data they have collected since the last update.

Immediately one asks – what data? In-car navigation systems use GPS to locate themselves. That means they can also track where they go, at what times, and

through this data one can easily establish interesting information such as speed. One possible use of this data, when harvested from many individual devices, is that TomTom can deduce where bottlenecks might occur at various times, and use this deduction to navigate around a bottleneck rather than right through it. However, TomTom did more. They also provided the data to the government – ostensibly for use in road and traffic planning so that bottlenecks could be cleared through better road design and traffic engineering. The problem is that the government found another, darker use for the data. Handing it on to the police, the data was then used to identify locations where drivers generally showed a propensity to exceed the posted speed limit. The police promptly set up mobile speed cameras and harvested windfall fine revenue for the Dutch government.

In all probability, TomTom did not foresee the use of the data by the police, and the police probably saw the data as an opportunity to deal with a problem – even if the problem was not one with which the general public identified. But the event does highlight that, regardless of the extent of information security, the behaviour of people can result in misuse of data that has come to them via legitimate means. Part of improving information security comes with improving the attitude of people to the data over which they have stewardship.

The **iPhone Tracker** issue has some similarity to the Tom-Tom Furore. It was revealed in April that some iPhones keep a log of where they have been as well – enabling post-event tracing of the owner's movements and raising many privacy questions. After initially denying the existence of the feature, Apple subsequently acknowledged that the retention of location data is a design feature intended to improve performance of the phone as it moves from one base station to the next. The problem arises when the data required for the internal design feature is stored in a generally accessible location and can be readily copied to other devices, at which time it can be easily analysed and used for inappropriate purposes. While Apple has dismissed the situation as a "bug", it does again highlight the tendency for software designers and builders to take shortcuts and give insufficient regard to information security as a first priority – creating the risk of exposure in the first place.

My **Email from an Airline** came just a few days ago – after I joined their frequent flyer program. Having selected my user name and carefully chosen a suitable secret PIN (Personal Identification Number) which was entered twice to make sure that I didn't mis-key it, the airline then very kingly sent me a welcome email with, you guessed it – my user name and PIN prominently highlighted, in clear text.

Long term readers know that I have a significant problem with this behaviour and have commented on it before. But while it's a bad thing for mailing lists to do it, it's absolutely inexcusable for an airline, which is as part of my membership also holding significant personal identification data, such as my passport number!

I immediately wrote to the airline to express concern and surprise. They responded promptly by advising me that they "are not allowed to disclose any membership information to anyone except the main member". This reply showed that at least the person on the service desk fundamentally did not understand that the breach was not one in which they would be voluntarily giving my information to another, but that they had already exposed login information that would enable an unauthorised person to access my details without their knowledge, or mine.

My email to the airline had pointed out that most email messages are fundamentally insecure documents – rather like postcards. Emails can be copied, stored and viewed at several points during transmission from sender to receiver. But all of this happens inside the machines, which most users of information technology don't understand. For the majority of users, an email would seem to be a magical transfer of text from one screen to another, without any intermediate steps. The human behaviour is to simply be oblivious to the detailed workings and therefore to simply not comprehend the associated risk.

How do we solve this problem? Frankly, I think it's less of a software design issue than one of fundamental education supported by better system designs. Secure email transmission is possible, to an extent, but it's clunky. It can be made much easier to use, even to the point of being completely transparent to the ordinary user – if only we choose to set up our email systems that way and carry the cost of the more complex setup and transition. But while we are thinking about that, surely we can also start some education programs – in workplaces, in schools, in social and business networks (both old fashioned meeting based networks and new-age online networks), and using the media. Experience has shown that television advertising does work to change society's attitudes to issues such as drink-driving – perhaps we should be thinking about similar campaigns to introduce new behaviours for safe online communication. [top]

Rocks Hiding in Clouds

Cloud Computing is one of the latest, greatest examples of IT industry "hype". Everywhere we see vendors, analysts and journalists exhorting "the Cloud" as the answer to the IT infrastructure needs of the world. Like all fashion, if you're not in the cloud, you're out of date. Cloud is touted as being more economical than owned infrastructure, and as removing barriers to new systems through virtually

instant access to flexible capacity through a mere touch of a credit card.

We all know that marketing hype always glosses over the downside. What's been interesting in the case of cloud computing is the intensity with which the conservatives who question the risk in the cloud are castigated and dismissed by those who promote its advantages.

If one believes the marketing hype, and even some of the serious analysts, the cloud is more reliable and secure than any in-house IT setup; but two recent experiences are now showing the falsehood in such extravagant claims.

For Infonomics, the cloud has been a fact of life for more than ten years (yes, we were in the cloud before the term became the latest darling of the marketeers) because we choose to have our email managed on a virtual server. That has saved us having to learn about, set up and manage an email server of our own, and get on with more important business. Over the years, the virtual server has moved physical bases several times, mostly with no impact on us. However, there have been a couple of incidents which showed us that living in clouds is not always easy. A few years ago, some outbound emails started mysteriously disappearing. It took a while, but we found that somebody had introduced an outbound spam filter that simply dumped any message containing defined "spam words". One of these defined spam words is contained inside the word "specialist". If you don't recognise it – drop off the first three letters, and the last – yes – a spam word and the reason why certain outbound messages were disappearing. Yes – we thought it was dumb too – but the cloud operator genuinely thought he was helping!

During the recent trip to the Gulf Region, Infonomics encountered another cloud problem. This time it was on arrival in Oman, when access to the Infonomics mail server disappeared. Through use of alternate email facilities, we were able to quickly establish that, again as a spam prevention measure, some bright spark in the cloud centre had decided to unilaterally block all access from any Oman internet address to all servers in the centre. It took three days to have that blockage removed, by which time I was back in Abu Dhabi and wading through hundreds of banked up messages.

But one company's misfortune in the cloud can be attributed to many things other than the cloud itself. What really grabs the attention is when there is a major failure in a cloud service provider, and a major incident of this type occurred with the cloud service provided by Amazon on April 21st. The prolonged failure of Amazon's Elastic Compute Cloud (EC2) impacted many organisations – some of them quite substantial, and left them powerless to resolve the problem while Amazon worked on fixing the failure.

There are numerous news articles and commentaries already in circulation regarding the Amazon failure. One highlights the caution expressed by the Australian Government Information Management Office which in January 2011 questioned the potential for loss of control of data stored in the cloud, and the possibility of a data breach in the public cloud. Certainly the Amazon incident brings at least the first of these issues to the forefront, with an admission that a small, but still significant 0.07% of data storage volumes attached to the virtual servers it hosts will "never be recoverable". Other articles highlight that many businesses have been disrupted at least from an operational perspective – Amazon's cloud service being down meant essential business systems became inoperable and some business activities were stopped!

Despite the pitfalls illustrated by the Amazon case (and amplified by the Epsilon data breach discussed earlier – Epsilon being an example of that part of cloud computing more commonly known as Web 2.0, or SaaS – Software as a Service), it is unlikely that cloud computing or the hype surrounding it will go away any time soon. Indeed, Cloud Computing is little more than the latest generation of the shared computing concept that first emerged in the 1960's when IBM released operating systems for its mainframe computers that allowed them to make one mainframe appear as several individual "virtual machines". This allowed the already-present computing bureaus to extend their "one customer at a time" shared use of a machine to a "several customers at one time" model. Thus, while the concept has waxed and waned over time as new and more compact technologies have emerged, the only thing that has really changed in cloud computing in recent times is the complexity of the underpinning technology, the scale (both upward and downward) of what can be placed into the cloud, the geographic and jurisdictional dispersion, and the nature of the contracts.

Think about that complexity for a moment. David Rice, in Geekonomics, points the finger directly at software complexity and the lack of engineering rigour in software development as one of the reasons we have so much trouble with information technology today. Can anybody really convince us that the additional layers of software complexity involved in cloud computing (on the service delivery side) make us safer? Amazon's own statements show that the work to repair the problem took "considerably more time than we anticipated".

Ultimately, Cloud Computing involves a trade – we exchange convenience for risk and a loss of control. The extent of risk and loss of control varies depending on how we choose the cloud provider, and how we structure the deal. A "private cloud" as promoted by some major companies reduces the risk of losing control, but it does still carry the risk of higher

complexity on the supply side of IT while offering distinct advantages on the demand, or use side.

Most organisations will inevitably find themselves "in the cloud" – more than a few will probably be there without realising it. While the benefits can be significant, the risks can also be considerable, and thus board should ask deep and significant questions about the organisation's approach to cloud computing. These might include:

- What cloud computing, software-as-as-service and other Web 2.0 services is the company already using, and to what extent is this use covered by appropriate internal policies regarding use of such services (caution: IT managers may not be fully aware of the extent of use of such services, as business personnel may have bypassed IT controls to directly access such resources via the Internet)?
- What of the company's information is stored in external facilities such as cloud computing, software-as-a-service and Web 2.0 environments, and to what extent is this information at risk of unauthorised access, loss or damage? To what extent is this information now subject to the undesirable and inappropriate judicial reach of foreign nations and to what extent is it now inappropriately beyond the legitimate judicial reach of nations in which we operate (Caution: Again, IT managers may not know all of the answers here – business users are quite often capable of moving data outside the organisation without the IT team being aware)?
- Which of the company's business systems are dependent on cloud computing, software-as-a-service and Web 2.0 services to an extent that a failure of such services will significantly degrade our business capability?
- Where the company is using, or proposes to use cloud computing, software-as-a-service and Web 2.0 services, what is the business case for doing so, and what specifically is the balance between value derived and the risk associated from ceding of control?
- Are the policies we have established and the controls we use sufficient to ensure that any use we do make of cloud computing, software-as-a-service and Web 2.0 services does not result in unacceptable risk to our business and legal obligations regarding privacy, accessibility, integrity and accessibility of information, or to our ability to sustain normal business operations? [top]

Gartner's Eureka Moment

Recently I discovered a Webinar published by Gartner Group on the subject of "Business and IT Governance Alignment to Drive Impact".

To be quite honest, I've long been cynical about Gartner – too much of their research has seemed to me to be focused on telling us what everybody is already doing, and not enough on opening our eyes to the future. They have also seemed very beholden to "establishment" views of IT, and not adventurous in promoting a wider range of insight. In respect of governing IT, Gartner held on for too long to the narrow, decision making arrangements focus presented by Weill and Ross in their 2004 book on "IT Governance", and when they did eventually move to a view that was aligned to ISO 38500, it was with no acknowledgement of the standard at all.

But now I have to admit, they have surprised me with the extent of insight and perspective shift demonstrated in this webinar. While it takes a few minutes to sign up as a (free) Gartner user, and while the presenter is sometimes annoying with his frequent bursts of "um, um, um, um, um", the hour long session does contain some very significant and relevant messages.

Gartner's core theme is very closely aligned to messages that Infonomics has been pitching for several years now – that governance of IT is not about the IT, but about the business use of IT, and should not be focused on the technology itself but on the effective use of technology in business change and operations. Gartner stops short in this session of the operational aspect – their focus is very specific to business change, and in this context they are clear and specific – governing business change means governing all the resources that are essential to business change – including the IT resource. For me, this is Gartner's Eureka moment – their realisation that governing business change involves much more than just the IT element.

In focusing on the resources required for successful change, Gartner has extended its Eureka moment by identifying Executive Attention as one of the most critical, yet scarcest of resources. Infonomics has long held, and in his 2004 thesis Dr Raymond Young demonstrated, that top management attention is critical to the success of what we persistently, if inappropriately call IT projects. Not only does Gartner now recognise and promote this criticality, they provide a delightful example of how one organisation – BT (British Telecom) addresses it: If a business executive fails to give appropriate attention to a project in that executive's domain, the project is terminated immediately!

In the webinar, Gartner goes on to highlight the absurdity of trying to configure governance around technology domains. They emphasise that governance of IT must be driven from a business perspective and that if it must be divided into domains, those domains should be structured around the business model, using tools such as a Porter Value Chain. Infonomics experience of implementing ISO 38500 aligned governance arrangements is that segmenting business focused governance of IT along the value chain (as long as it is not excessively segmented) is extremely effective and promotes very

strong engagement of business leaders in setting the business agenda for effective and in some cases quite innovative use of IT.

Following this same line of thinking, Gartner also points out that if an organisation establishes a Program Management Office, it should focus not merely on risk associated with the IT resource, but on the whole of business change risk, paying attention to the full set of scarce resources.

Finally, Gartner dispatches one of the trickiest questions coming from organisations today – regarding the value of IT. They point out that value is indivisible across the resources consumed in its creation. Business change creates value by integrating executive attention, financial resources, human effort, information technology resources, organisation design, process design and other intellectual property. Removing any of these essential ingredients does not reduce the value of the change – it fundamentally destroys it.

No doubt these views will be further developed in the future. [top]

Infonomics Education Program

The Infonomics education program continues to draw substantial interest, especially in the international arena.

Two day ISO 38500 Foundation Class

Brisbane (Australia)	Bookings closed!
Sydney (Australia)	Bookings closed!
Kuala Lumpur (Malaysia)	June 6/7

One day ISO 38500 Immersion Class

San Salvador (El Salvador)	May 24
Buenos Aires (Argentina)	May 26

ISO 38500 Introductory Briefing

San Salvador (El Salvador)	May 23 (in Spanish)
Buenos Aires (Argentina)	May 27 (with the National Office for Information Technology for Argentina).

For more information about events in San Salvador and Buenos Aires, please contact BITCompany.

For events in Malaysia, please contact Expitris Worldwide Sdn Bhd. [top]