The Infonomics *Letter*
Plain Language about Corporate Governance of Information Technology
May 2010 Edition

Advancing the Agenda

Welcome to The Infonomics Letter for May 2010.

Last month, we published the summarised results of the international survey into governance and management of IT. The report has been the subject of widespread discussion and commentary, having been referenced in several blogs and other journals. It's also been discussed at length on the business networking site, LinkedIn, where its availability was publicised to several groups interested in boardroom activities and in the specifics of governing IT. Perhaps unsurprisingly, there is little effort to rebut the findings – it seems that many accept that the current capacity of boards and executive teams to govern IT is relatively low. Much of the debate has gone to how we resolve the problem, with many leaning to the desirability of having IT specialists on the board. Frankly, this approach is wrong. Discover why in **Developing the Board**.

Recently, Standards Australia published a new companion to ISO 38500 and its predecessor, AS/NZS 8015. The new standard, AS/NZS 8016:2010 addresses "Corporate Governance of projects involving investment in information technology". See more in **AS/NZS 8016 – Oversight of Projects.**

As more and more of the routine processes of organizations become infiltrated by supporting information technology, so too are we more frequently hearing of things going wrong, with the reported cause being a "computer error" or a "computer malfunction". But how often are those problems truly a result of a computer system just losing the plot? How often are they actually a result of a human error that the computer system has not recognised? In **Fat Fingers or Fatal Flaws** we explore how some organisations seem to build computer systems expecting that their human operators are infallible.

May has been a very hectic month of standards meetings and briefings. First I was in Helsinki for a meeting of the international working group focused on further developments in guidance on governance of IT. There we looked at plans for the next generation of ISO 38500, development of the overall model for governance and management of IT, and further implementation guidance. Then it was off to London, Amsterdam and Brussels for meetings and briefings – further expanding the ISO 38500 community of awareness. These meetings confirm that, ISO 38500 is capturing interest and imagination in major organisations that depend on IT, and in specialist services firms.

Mark Toomey
31 May 2010

Coming Events

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

June 1 - 3: International Green IT Awareness Week. This is a week-long virtual event, with sessions being delivered by webcast. It launches at 11:30 am Eastern Australian Time on Tuesday June 1. To register, go to the conference website. The conference schedule gives details of session times for global audiences. After initial delivery, sessions can be accessed on demand.

At 3:00 pm AEST on June 3rd, I will be delivering a session on *"Application of ISO 38500 to the Green IT Agenda".*

June 24 – 25: Kuala Lumpur, Malaysia: ISO 38500 Foundation Class, with Expitris Worldwide.

July 27: Dunedin, New Zealand: Institute of Directors Otago Branch and Otago School of Business: Board/Executive briefing on Governance of IT. More details TBA.

July 29: Auckland, New Zealand: Not for Profit CIO Network lunch briefing on ISO 38500 and governance of IT.

August 2 – 4: Melbourne, Australia: ISACA Oceania CACS 2010: Briefing on Audit and Governance of IT in a Post-Recession World.

October 5: Melbourne, Australia: ACOSM2010 - The Australian Conference on Software Measurement, in conjunction the International Software Benchmarking Standards Group's (ISBSG) Annual Workshop. I will be tackling something different – *"Measuring the Unmeasurable: Governance of IT".*

Developing the Board

According to recruitment firm Korn/Ferry International (as published in the Australian Financial Review in December 2009), company boards are often unable to understand and evaluate the investment required for large information technology programs. This observation is entirely consistent with the survey findings published in The Infonomics Letter for April 2010, where only 37% of boards were regarded as having effective oversight of their organizations' current and future use of IT, and less than 30% of boards were regarded as having the necessary skills and knowledge to provide that oversight.

In common with frequently-expressed opinion, the article suggests that there is "a need for more IT savvy on company boards". Indeed, the research conducted by Infonomics suggests that IT savvy is needed not just at the company board level, but also at the executive management level.

How does one add IT savvy to a company board? One of the most frequently cited methods is to add a director to the board who has deep IT experience. But is this appropriate? What are boards getting when they add an "IT expert" to their number?

A few boards have been able to acquire the talents of past top executives of IT companies – and thus can lay claim to having satisfied their need to have "IT expertise". These individuals undoubtedly have significant experience in running an IT company, but rarely will it be based on either deep technical skills or front line IT management skills. Their experience will be as generalists, gained as much from observation of, and engagement with their customers and from interacting with their own senior people as it is from their own direct experience of planning, implementing and operating the IT enablers for their organization.

Some boards have sought to fill the knowledge gap by appointing IT specialists – people whose career experience has been predominantly in the IT arena, such as past chief information officers. But, as one IT savvy director recently told me: "I believe that even when companies put IT governance capability (specialists) on boards, the other directors may not really understand the issues and therefore not participate fully or at all leaving the IT person as a lone voice. As a lone voice, often it is not possible to make progress in a structured strategic way. Something has to be quite an issue for general agreement to happen".

The distinction between the two approaches to adding IT savvy through specialist recruitment is perhaps a significant indicator of where the ultimate answer lies. The former approach of adding a generalist who has broad management experience and specific IT experience means that at least the new recruit should be familiar with the language of directors and able to lead the board conversation on IT matters, while ensuring that at least the majority of the directors are engaged and understanding the key issues. The latter approach of adding a specialist might result in directors remaining "in the dark" and unable to make a properly informed judgement.

Directors need to make judgement on many issues in the normal course of their duties – about finances, risk, legal matters and so on. In virtually all of these areas, in most organizations with effective boards, all of the directors are able to participate in the discussion, ask relevant and incisive questions, and make informed judgement on the issues. Yet, while most boards include individuals with in-depth expertise in accounting, the law and other disciplines, discussion of these issues is not restricted to the specialists. In fact, the discussion is generally one of experienced generalists, where one or two may have an in-depth expertise which can be drawn on and comprehended by the generalists.

Look at formal training for company directors. The well-known "Company Director's Course" run by the Australian Institute of Company Directors includes modules such as: "Risk - Issues for Boards"; "Strategy - The Board's Role"; "Financial Literacy for Directors"; and "The Board's Legal Environment". These modules (the author has completed the Company Directors Course) recognise that while directors cannot be specialists in each of the disciplines, they do need a generalist capability to understand and interrogate the information they are being given by management, so that they can make informed judgements.

With information technology now being pervasive in its integration with the current operational business systems and future capabilities of most organizations, the issues for directors are not ones of deep technology debate. They are more general in nature – focused on whether the IT is being used effectively, whether the risks are properly understood and addressed, and whether the investments are likely to deliver the intended outcomes. Just as in accounting and legal issues, the desirable expertise of the director is not that of the in-depth technical specialist, but rather that of the broadly capable and well-informed generalist, who knows broadly what should be happening, can ask questions to elucidate when the wrong things seem to be happening, and can refer areas of doubt to suitably qualified specialists.

Just as the majority of directors can build on their past management, consulting and other careers to build a competence in established fields like legal and accounting, so too should directors be able to build an appropriate level of generalist expertise regarding the use of information technology.

This monthly Infonomics Letter and the book, Waltzing with the Elephant, are just two of the resources Infonomics provides to help directors who have no prior experience with IT develop the broad general understanding they need to comprehend, ask questions and get expert advice when dealing with their organization's current and future dependence on the information technology resource.

Further resources are in the pipeline.

AS/NZS 8016 – Oversight of Projects

When the original Australian Standard AS/NZS 8015 was published, there was an expectation that it would be followed and complemented by a series of additional standards and other guidance on governance of IT in particular contexts. At the very least there was intent to publish additional standards

on topics that were at the time referred to as "IT Projects" and "IT Operations".

Developing a standard to advise directors and top management of organizations on governance of "IT Projects" proved extremely challenging. But after more than five years of effort, an interim standard has finally seen the light of day.

Now named "Corporate governance of projects involving information technology investments", AS/NZS 8016:2010 was published as an interim Australian and New Zealand standard in February. Following the model established by AS 8015 and the current ISO 38500, AS/NZS 8016 is a brief document of just 16 pages, setting out a model and principles for governance of projects, and designed for use by directors and those who advise them.

The choice of name for the standard is important: it seeks to ensure that organizations focus on the complete initiative required to deliver intended business outcomes, rather than merely on the IT elements within the initiative – the elements that are sometimes referred to as the "IT project". AS/NZS 8016 takes as a fundamental premise the notion that is often verbalised as "There's no such thing as an IT project – just business projects that use or depend on IT".

Like ISO 38500, AS/NZS 8016 does not prescribe any management framework or methodology for projects. Rather, it exhorts organizations to employ relevant frameworks and methodologies, or parts thereof, as and when relevant to help them ensure that they have adequate management systems in place.

AS/NZS 8016 provides a succinct definition: Corporate governance of projects involving IT investment is the system by which projects that involve investment in changed or new IT capability are directed and controlled, from initiation to the achievement of the business outcomes. This definition is important for several reasons – and especially because it makes it clear that the governance oversight must continue until the intended business outcomes have been achieved – or of course until it is obvious that they cannot be achieved in which case the project should stop. The standard also reinforces the use of the term "project" in its generic context, as an organised undertaking intended to produce an outcome. This is the language and context that is widely used in boardroom and generic conversation about major investment undertakings, and avoiding the specialised and sometimes confusing narrow technical terminology of the IT community.

Inside AS/NZS 8016, the model and principles presented in ISO 38500 are carried over and amplified in the specific context of projects. The Evaluate – Direct – Monitor model continues, and these tasks are now explained in the more specific context of projects. Similarly, the six principles are carried over (though for clarity, Principle 3 is renamed from "Acquisition" to "Investment"), and expanded upon by more in-depth discussion of their meaning in the context of projects. The discussion includes identification of desirable behaviours – the things that organizations should do in conforming to the principles. These behaviours should provide a useful lens through which directors (and other stakeholders) can check and verify that management is doing the things necessary to assure success of the initiative.

While AS/NZS 8016 has been the product of an enormous effort, there is more work to be done. The governance concepts, while indelibly tied to those expressed in ISO 38500 and likely to strike a chord with those who normally operate in the boardroom, may be less familiar to IT and other project specialists who are accustomed to substantial process based methodologies. Early experience in application of the standard is likely to produce further learning that should be reflected in an early update, which should then further advance the state of the art. For this reason, AS/NZS 8016 has been published as an interim standard, which will expire two years after its first release. During that two year period, Standards Australia will collect comments from the public, with these comments contributing to a determination as to whether the current document will be confirmed, revised or withdrawn. This two year comment period, of which one quarter is already expired, provides the opportunity for collection of extensive practical experience and further development of theoretical knowledge on the topic.

While published as an Australian and New Zealand Standard, AS/NZS 8016 should be of interest to the international community, as it builds on the guidance provided in ISO 38500, and should help those adopting ISO 38500 to build a more complete understanding of its intentions.

For more information and to purchase AS/NZS 8016, refer to the SAI Global website.

Fat Fingers, or Fatal Flaws

How much impact can a simple typing error have? During May 2010, the world's financial markets reeled once again as the Dow Jones industrial average plummeted. But this time, the trigger was not a repeat of the bad economic data and associated panic we recall from October 2008 (although the markets were nervous about Greek debt and were therefore highly sensitive). Instead, it was what traders euphemistically call the "Fat Finger Problem".

Quite simply, the fat finger problem happens whenever a person enters incorrect data into a computer system, and the system blithely accepts the data without a blink, even when there is plenty of context to suggest that the data may well be incorrect!

Fat Finger can happen to anybody. Not too many years ago, I found myself pleading with my bank and

one of my suppliers, because in making an online bill payment, I managed to omit a decimal marker and inadvertently overpaid the bill 100-fold.

Sometimes fat finger can just result in inconvenience and additional cost. Sometimes, as demonstrated in the Wall Street case, it has the potential for significant impact on society. Sometimes, it can be fatal.

In March 2009, an Airbus A340 carrying more than 200 people narrowly escaped disaster at Melbourne Airport after the flight crew entered the wrong take-off weight into the plane's computer. As a result of the aircraft's weight being understated by more than 25%, the computer-controlled engines were programmed to a low thrust level that would not provide take-off speed until the plane was well past the far end of the runway. Only the robust engineering of the aircraft and the power of its engines were enough to avert disaster when the captain over-rode the computer to select maximum power just before the plane ran off the runway. As it was, the aircraft struck landing lights at the far end of the runway, and was severely damaged as a result of its tail striking the ground.

These examples of "Fat Finger" reveal a weakness that has crept into systems that increasingly rely on information technology and which have removed layers of human intervention. On Wall Street, before online trading, a trade would have passed through several pairs of hands before final execution – and any one of those hands might have detected a likely error in the specified price. On a commercial jetliner, engine power would have been determined by the pilot in command and confirmed by the co-pilot – perhaps with a third check from the flight-engineer on those aircraft which still require such a role. But in automating systems, we seem to have forgotten that human beings are prone to error, and we have taken out the safety checks that were once an integral part of the process.

It's not always been that way. In earlier generations of information technology use, particularly when the IT was mainly used to automate and speed up repetitive activity, the designers of systems went to great pains to remove human error and therefore to reduce the likelihood that costly problems would creep into essential business activities. Methods such as batching of input data and calculation of control totals were highly effective, if tedious methods of ensuring that all of the required data was captured accurately. Extensive validation protocols were used to limit the potential for bad data to get into systems.

But somewhere in the last wave of automation, where IT has been integrated directly into the front-line business process, there seems to have been a loss of recognition that human beings make mistakes. In many of the all-too-frequent press reports of things going wrong with computer systems, the trigger is a human mistake in entry of data – and no matter how many attempts are made to write the situation off as a "computer error", the reality is that the problems occur because organizations do not put enough effort into understanding where their key business systems are vulnerable to human error.

The Wall Street error could have been easily detected and resolved. The trade price entered was dramatically out of accord with prevailing conditions and was most likely to be wrong. An intrusive check, which demanded that the trader stop and think, should have been triggered by the systems – exactly as would have happened if the trade chit had been handed off to a clerk.

So too with the Airbus (comprehensive information on what happened with the Airbus can be found at the Australian Transport Safety Bureau). While the weight specified might have been correct for an otherwise unladen plane on a test flight, it is highly unlikely that it was within normal range for an operational flight. At the very least that check should have been triggered. Perhaps, as with many other aspects of aviation operations, there should have been an enforced requirement for confirming input from both pilots. And, thinking about other systems on the aircraft, there might have been cross-checks with fuel gauges (full tanks might indicate a probability of significant load). Going further, in this modern era of global positioning systems, might the take off control computer have constantly checked if the aircraft was accelerating strongly enough to take off before reaching the end of the runway? Just how many ways might a little more investment in safety have trapped and prevented this near disaster that was a product of human behaviour?

Directors of most organizations should regularly ask questions about which innocent human errors could have major negative consequences, and satisfy themselves that the associated information technology is effective in trapping these errors before they become disasters.

Waltzing with the Elephant

Waltzing with the Elephant is Infonomics premier resource for board directors, executives and IT specialists who want to achieve effective top level governance of IT, maximising value and effectively controlling the risk of investment in IT. Based on more than 30 years of practical experience, and ten years of focused attention to governance issues, Waltzing with the Elephant has enjoyed critical acclaim from a wide spectrum of reviewers in boardroom, executive, IT and consulting roles. A selection of reviews and a preview of the book are available at the Infonomics Website.

Waltzing with the Elephant is a publication of Infonomics Pty Ltd, and is available for purchase from The Infonomics Shop in paperback and downloadable e-book editions.