The Infonomics *Letter*
Plain Language about Leadership and (Corporate) Governance of Information Technology
January 2011 Edition

Looking ahead and growing

Welcome to the first Infonomics Letter for 2011. After a seven week break and a series of amazing weather events across Australia and in other parts of the world, we are ready once again to explore and promote good practice in governance of IT.

Working as an evangelist for new thinking about anything can be an interesting task. Being an evangelist for a new way of looking at governance of IT involves challenging many established beliefs and methods of operation. But while the road is long, arduous and, in the short term at least, hardly viable from a financial perspective, it is gradually unfolding with evidence of change. Not so long ago, the mere suggestion that directors of organizations should ask questions about IT would once have spurred horrified denial that directors could ever understand the topic. Yet now, at least one major bank in Australia has a board committee to oversee its extensive agenda of IT change.

Recent events, several of which have been discussed in The Infonomics Letter through 2010 are leaving no doubt that business dependence on IT is now, in many cases, absolute. Now, when significant problems occur with IT, it is almost axiomatic that the top line of the organization's leadership gets involved, and this presents a context in which we can see that business leaders need to know things about IT that may not in the past have seemed relevant. Peter Grant, a well-known Australian IT industry researcher and commentator brought this into focus in a recent post to a LinkedIn discussion forum, and the Infonomics response to his challenge is presented in *What Should Management Know*?

Of course, the shift to a new year does not stem the tide of case examples where a small dose of effective governance might have avoided embarrassment and perhaps other consequences. This month in *More Red Faces* we explore the stunning revelations of weak information security at Vodafone Hutchison Australia, and postulate a governance approach based on ISO 38500 that might have saved the company from being lashed to the whipping post during the usually slow news period in mid-January.

The new government in Victoria is beginning to flex its muscle, looking deeply into the unfulfilled promises of the previous government's major IT initiatives and asking "is it worth it"? We foreshadow further scrutiny in *New Opportunity to Improve.*

Finally, there's news of how Infonomics commentary now appears on Delimiter, major advances for Waltzing with the Elephant, and the near term education program.

Mark Toomey 25 January 2011

What Should Management Know?

LinkedIn is an online networking forum for professionals. Among its readily accessible facilities are the discussion forums, or groups, where individuals with similar interests share and debate news and ideas.

The Australian IT Industry group on LinkedIn has more than 15,000 members. One discussion, launched in April 2010, asks *What Are The Things We Hate About IT?*

The discussion builds on a blog post entitled *Eight Things We (Still) Hate About I.T.* by Harvard Business Review writer Susan Cramm. It's generated strong debate, including several posts from IBRS researcher Peter Grant. Peter has held a number of quite senior roles in research, government, academia and the IT industry. He isn't afraid to say what he thinks and, while I don't necessarily agree with all of them, his posts often give good food for thought.

Just a few days ago, Peter posted the following challenge: *What exactly should management know about IT? Let's have a discussion about that with some concrete examples.*

Well that's a pretty good challenge, and one that presents a useful way to launch The Infonomics Letter into 2011. So here's what I think.

First and foremost, the term "management" in this discussion refers to business leaders. I'll extend that to include, where relevant, the board of directors or other governing body that may exert direction and control over the organization.

Above all else, management should know that IT is a resource that has become intrinsic to the ongoing operation and future capability and performance of their organization. As an integral resource, regardless of any other consideration, IT cannot be treated in isolation. Nor can IT be eliminated from the business of management. IT is critical, as has been amply demonstrated in the recent cases of Virgin Blue (*Oops, Sorry!* September 2010) and the National Australia Bank (*The Red Faced Bank*, Nov/Dec 2010). When IT goes wrong, the business impacts can be profound, and regardless of the supply side issues, business management has a fundamental responsibility to ensure that the business systems operate as they should, and when they should.

Management should know that, as with all resources, achieving objectives depends on how the resource is used as well as on how the resource is supplied. In manufacturing, a great supply chain will be worth little if it is feeding an erratic and inefficient production process. In IT, a highly developed IT supply capability is equally worthless if it is matched

to ineffective business use of the IT. Equally, as illustrated in the examples quoted above, having a great business that is not matched by great IT supply can have devastating impact.

In order to make efficient and effective use of IT, management must know how its business works, and particularly, how to implement change in the business. H.J. Leavitt's mid-1960's work on organizational change (*Applied organizational change in industry: structural, technological and humanistic approaches*) shows that managers need to understand four elements of their business system – the people, the tasks (processes) they perform, the organization structure and rules under which they operate, and the tools (technology) that underpin the system. Leavitt's work should leave no doubt for management that attempting to implement change enabled by IT must take an omnibus approach, simultaneously addressing all of the elements of the business system. Sadly, we continue to see case examples where there has clearly been a disconnect – a naïve expectation that the IT project can lead change and everything else will work – a recent example being the 2010 case of Queensland Health, which is discussed in the June 2010 edition of The Infonomics Letter.

The current and future capabilities of IT are now fundamental to competitive positioning of many organizations. Those which miss the opportunity to exploit a new IT-enabled business capability or opportunity may find themselves being overrun by more insightful, more agile competitors. This situation is very clearly demonstrated in the current campaign by some Australian retailers who are seeking a removal of tax emptions for certain goods purchased online from offshore suppliers. The retailers complain that they are losing business because shoppers are buying online, but more careful scrutiny of the situation reveals that the price differentials are not merely a product of tax savings. Rather they are the result of the profound difference between an online business model and the numerous inefficiencies of the old style shopfront and warehouse approach to retail.

It is this business-critical context to which the international standard for governance of IT is directed. Where much of the discussion about IT has focused on the limitations of the supply side, and many of the frameworks and tools have focused on improving the performance of the supply side, ISO 38500 is fundamentally based in the realisation that the value in use of IT comes from how, where and when it is used – the demand side. Once they understand that IT is key to the ongoing performance of the organization, business leaders should also understand that they can and should direct and control the use of IT, and that ISO 38500 shows them how to do so.

ISO 38500 says that organizations should evaluate, direct and monitor the organization's current and future use of IT. While ISO 38500 assigns these tasks to the governing body, it also recognises that the majority of the effort required will, necessarily and correctly, be delegated to management.

To evaluate the use of IT, management must first understand how the business operates and how it uses IT. Management must then consider how the business could operate, and how it could use IT. Evaluating the current use of IT includes considering whether or not the existing IT platform and capability are fit for purpose and how long they will remain so. The assessment process and criteria are similar to those which would apply to physical plant and equipment. Questions relating to life expectancy, maintenance costs, availability of skilled workers and spare parts all come into play. And just as evaluating plant requires sound knowledge of the purpose and operating characteristics, but little knowledge of design and construction of individual machines, so too does evaluation of IT focus on external rather than internal aspects of the technology.

Evaluating the use of IT can also include evaluating the supply capability and future options. These questions must go hand-in-hand with fundamental questions about the business – how agile it needs to be; how much risk it is prepared to take; how close to the leading edge of innovation it intends to operate.

Directing the use of IT means much more than preparing a forward plan of projects to be undertaken. It means establishing clear rules by which the organization operates in respect of IT. It means establishing appropriate business oriented targets for the use and supply of IT, and implementing control mechanisms to keep these targets at the centre of attention. The targets should be oriented as much to business operational matters as they are to the value to be realised from new investments.

Because IT does not stand alone, directing the use of IT does not focus only on the IT elements of the business systems. Rather, directing the use of IT should be an intrinsic element of directing the business. In planning new business capability, attention must be given not merely to the raw potential of the technology, but to the impact of the technology on the entire organization, including its customers, suppliers, internal personnel and other stakeholders, as well as its plant and overall infrastructure. In building new business capability, the need is not merely to acquire, build, test and commission software, storage, servers, communications and desktops. Rather it is to progressively transform or build entire business systems comprising people (many of whom may not be employees), processes (some of which may be

integrated upstream with suppliers or downstream with customers, or outsourced), organization structure and rules (which may be geographically dispersed, transcending national borders, legal jurisdictions, time zones and climates), and the technology that enables the entire system to operate. From an operational perspective, it includes establishing standards for life-expectancy, resilience, flexibility and a raft of related parameters that again are not merely technology questions but fundamentals of how the business operates.

Few organizations operate in a static environment, and even fewer have perfect ability to follow a set direction without some variation. Thus, monitoring remains an essential discipline in top level management and board control of the use of IT. However, the monitoring that is required is not merely low-level monitoring of IT equipment and systems performance. Rather it should be focused on understanding the part played by IT in the ongoing operation of the business. Matters such as cost and profitability of a business transaction are generally important. The difference between current average and peak business workload compared to the theoretical maxima for sustained and burst workload are significant in meeting increasingly demanding customer expectations and provide a context in which the raw measures of IT are presented in the light of other factors that can influence overall business results. Understanding that IT is just one of the factors that can influence performance is essential to efficient business level capacity management. Factors that influence business operations and activity should also be in scope for monitoring – alerting the organization to forthcoming changes in environment and other circumstances that may significantly alter its activities and expectations of IT in the short, medium and longer terms. Ability of the organization to achieve its goals can also depend heavily on the consistency with which the organization and particularly its managers conform to the requirements laid down in the rules that govern its activities. There should be an ongoing evidence based regime of confirming that the rules relating to the use of IT, as well as all other relevant rules, are both understood and observed.

Simply having visibility of performance and conformance is insufficient. Organizations unable to act appropriately on information gain no benefit from having the information in the first place. Management should ensure that the monitoring capabilities are complemented by mechanisms that result in timely and effective response. Robust examples of the need to be aware of changing conditions and to respond promptly have been evidenced quite recently in respect of the floods that have occurred in Queensland and Victoria. While the flash floods that devastated Toowoomba and the Lockyer Valley gave no warning and no opportunity to take precautions, the delayed impact on Brisbane, and the almost glacial progress of the 3,500 square kilometres of water in north-west Victoria have meant that communities, businesses and individuals have had time ranging from hours to days to prepare for the inundation.

ISO 38500 provides further guidance, by way of six principles. In most organizations, management should bring these principles to life by establishing clear policy that defines how the organization will behave. We have discussed the principles numerous times in The Infonomics Letter, and no doubt will do so again in the future. In short, management should:

- Assign clear and unambiguous **responsibility** for use of IT, with top level business managers having primary responsibility for effective, efficient and acceptable use of IT. Supplier responsibilities (including those of internal IT functions) should be equally clear and delimited by the actual capability of the supplier. In particular, suppliers do not generally plan the business, implement organizational change, or run the operational business. Naturally, those who are assigned responsibility should be competent to perform the role, and accountable for its corresponding outcomes.
- Ensure that the **strategy** and plans for use of IT are integral to the business plans and are and that strategy and plans for supply of IT are congruent with the business plans. The business strategy should be informed by a clear understanding of the current and future capability of IT, as it exists within the organization and as may be possible through external developments. The capability dimensions to be considered include the obvious ones of functionality, as well as the less immediately obvious ones of how customers, suppliers and competitors are using technology, the availability of suitable supply arrangements to give access to technology, and the capacity of the organization and its stakeholders to assimilate IT-enabled change.
- Subject all decisions regarding **acquisition**, retention and disposal of IT to appropriately rigorous analysis, to ensure that there is proper balance of cost and value returned, risk and competitive advantage. These considerations should include a wide range of factors including maturity of technology, availability of expert skills, scope of change impact, business criticality, external imperatives and context of the particular item in the overall operational and investment plans of the organization. The analysis should apply equally to new investments and to routine expenditure, the latter being to ensure that routine

expenditure is in fact warranted in the context of the organization's longer term plans.

- Adopt a broad perspective on **performance** of IT, anchored in the performance criteria that are important to the business. Management should ensure that there is a robust, risk based approach to identifying and resolving IT-linked constraints on business performance, whether they relate to business throughput, business sustainability, stakeholder (customer, supplier, employee, regulator etc.) confidence, and business evolution.
- Assure an appropriate level of **conformance** to external and internal rules governing the organization's business activities and use of IT. Management should ensure that there is appropriate balance of education, automation and enforcement to promote an acceptable level of conformance to rules. In some organizations, this may need to be complemented by formal means of detection of, and remediation for, breaches.
- Understand that **human behaviour** is a key consideration in successful use of IT, at every point of engagement in planning, building and running an IT-enabled organization. Factors such as ambition, fear, ignorance, greed, along with the desires to be helpful, to avoid consequences, to be valued, and to tinker can all play a part in determining the success or otherwise of IT at any stage.

Peter Grant's challenge includes Peter's own initial list. The above discussion on how management should treat IT as a key business resource, and how management should use ISO 38500 to guide the organizations approach to directing and controlling its use of IT, provides a lens for some further discussion of his list.

(1) They do need to know that more often than not they don't need tailored software written for them and they probably don't want to be in the software development business.

This goes to the **strategy** and acquisition principles. With many software products available today, there is indeed little need for the cost, risk and time required for custom development, especially in aspects of the business which are not the focus for competitive advantage. To complement this knowledge, they also need to know that customizing of software packages can be ultimately more expensive than a tailored development, depending on extent of change, short and long term availability of skills, and the maintenance regime attached to the software product. Further, business leaders should understand that adopting packaged software also generally means adopting and adapting the business models on which the software was designed and that this can involve substantial expense and disruption in its own right. The impact and outcomes of this type of change may, in some cases, make selection of a package a poor choice.

(2) *They do need to know what IT costs them and what value they get from it along with alternatives for achieving the same outcome another way.*

This is absolutely consistent with the expectations of the **acquisition** and **performance** principles. But thinking about the principles should lead to a more expansive view. Management should go beyond understanding the cost and corresponding value of IT, to also understand the business consequences of under-spending, spending on the wrong things, and spending at the wrong time. The appreciation of value should go beyond the simple financial return on investment or expenditure, to consider any other value metrics that the organization has adopted – metrics such as sustainability, customer and employee satisfaction and so on.

(3) *They do need to have a measure of their organization's agility and identify areas that block rapid responsiveness (often it's IT doing the blocking).*

Again, this maps across several principles. **Strategy** should indeed be informed by a sound understanding of the organization's agility. **Acquisition** decisions too must take into account how much change can be tolerated, as well as how much can be delivered. Understanding and moderating **human behaviour** can result in quite different outcomes.

Peter suggests that IT can be a blocker to agility. This may be so, but many other factors can also obstruct progress with IT-enabled change. Resistance to change from line-of-business personnel, customers, suppliers and other stakeholders can be an impediment. Delay and cost can also be magnified when one is trying to build onto or adapt to an established IT environment that is way beyond its use-by date, or composed of ramshackle bits and pieces strung together as a result of unwise financial constraint on initial investments and subsequent maintenance. Too often here, the IT supplier is not the cause of the obstacle, but merely the messenger who has to (repeatedly) bring the situation into focus.

(4) *They do need to have a strategic view of security - it's not IT role to set this. IT tend to set security to make operations easier for them.*

Numerous illustrations are available today of organizations that do not take information security seriously. Peter is correct. Organizations should

clearly establish **responsibility** for information security at the top and cascading throughout the organization. Information security should be an integral part of the **strategy** of the organization. New and recurring expenditure on information security should be subject to the same rules for acquisition as other expenditure to ensure proper prioritization as well as confirmation of value and risk elements. Clear rules and **conformance** arrangements should inform all stakeholders of their part in information security, while ongoing assurance of security **performance** should, among other things, give specific attention to the **human behaviour** elements of the information security situation.

(5) *They do need to ensure they have access to timely and accurate information for making decisions.*

More than this, business leaders need to ensure that they fully understand the decisions that they must make. With IT now intrinsic to business activity, business leaders can no longer rely on IT specialists to fully comprehend the business context and accurately position the appropriate use of IT. Rather, as they develop **strategy**, business leaders must acquire and integrate into their thinking enough understanding of the capabilities and constraints inherent in IT to enable them to develop an appropriate vision and corresponding development paths for the organization. To be clear, the timely and accurate information that business leaders need is not limited to information about their business. It now includes information about how their competitors, customers and suppliers are using information technology, and information about the specific capabilities that are currently, or are likely to be delivered by IT.

(6) *They do need to know and understand the robustness of their overall organization - and since the weak link is often IT this needs constant vigilance.*

Regardless of what the weak link is, business leaders certainly do need to know how their organization operates and how robust it is. Changing circumstances can quite significantly and quickly change the level of resilience and flexibility. There are many cases where under-investment in and other poor controls over aspects of IT can greatly diminish capability to detect and resolve problems. Loss of corporate knowledge and essential skills through attrition, outsourcing and forced redundancy can, for example, have a dramatic impact on ability to detect and resolve problems. Equally, unrestrained ad-hoc introduction of new IT can result in fragmentation of key data, obscuring the comprehensive view of the business. Effective policy based oversight of IT use across the six principles can greatly reduce the likelihood of weak links developing or becoming entrenched, though ongoing monitoring is essential.

(7) *They do need to be constantly looking for ways to improve business processes and some of that thinking can come for effectively leveraging the benefits of new technologies - if their IT operations and security people let them :-) Just a little tongue in cheek but often they are a blocker here.*

As noted under point 5, business leaders do indeed need to be looking for ways to use IT to advantage. The search should not be limited to business process – it should deal with all aspects of the business model and the organization's business systems. Now, more than ever before, it is the vital task of business leaders to determine how IT is used, as part of determining the overall design and operation of the organization.

To remove the potential for obstruction to change, business leaders need to ensure that there is a very clear and balanced understanding of **responsibility** – which may be assigned quite differently now to the way it has been in the past. There should also be appropriate mechanisms in place to ensure that the organization's **strategy** for use of IT is sound, that each and every investment in, or **acquisition** of technology is appropriate, that all necessary aspects of IT **performance** are assured, that clear rules exist and are complemented by appropriate **conformance** arrangements, and that **human behaviour** is channeled to the best interests of the organization.

Long gone are the days when IT was confined to the back room and inconsequential for day by day activities of the organization. Also long gone are the days when IT could be regarded as an unfathomable mystery beyond the ken of a business manager. There is a discernible new flavour in the advice from a wide range of sources, emphasising that business leaders must play their part in directing and controlling their organizations' use of IT. ISO 38500 provides valuable guidance for business leaders, because its focus is on empowering them to direct and control the business use of IT without demanding that they become intimate with the intricacies of designing, building, integrating and operating the IT components. As the information era reaches an inflection point at which the infrastructure is rapidly disappearing into a cloud, ISO 38500 provides a new anchor for the ongoing and critical discussions about how the increasingly less tangible IT asset is used in an effective, efficient and acceptable manner, to create valuable business capability, with an acceptable level of risk.

More Red Faces

No sooner have we finished publishing stories about the transaction processing problems at the National Australia Bank, and before that the business disruption at Virgin Blue because of a server crash, and along comes the next case example. In somewhat of a coincidence, this company also has a prominent splash of red in its logo.

Vodafone Hutchison Australia (VHA) operates the Vodafone and 3 mobile phone and wireless internet networks in Australia. VHA is both a supplier of IT to its customers and a user of IT in the conduct of its own business.

VHA has been the subject of considerable customer dissatisfaction since around October 2010. Problems have been reported with mobile phone performance and wireless internet access. Regardless of how diligently or effectively the company was addressing the problems internally, the public remained unhappy, and a large contingent of VHA customers have taken up the issue using the internet. One Sydney based customer set up a website – www.vodafail.com – and attracted such extensive registration of problems that he has been able to compile a substantial report on the problems that has now been submitted to the national corporate and telecommunications oversight agencies. The weight of information collected provided a powerful incentive for VHA to meet with the operator of the website, in what would have been an essential public relations exercise. The collection of customer feedback is also likely to figure in a class action in which customers will be suing VHA in respect of the alleged performance failures.

But on January 9 this year, the performance failures and other complaints about VHA were pushed to the background by a newspaper report exposing what appears to be a massive lapse in security and privacy controls applied to customer data at VHA.

While VHA moved quickly to assure customers that their personal and private information was secure, other news reports also showed that it was scrambling frantically to deal with the weakness that had been exposed in the original report. Over the subsequent few days, the issue remained at the top of the news lists, and a variety of reports gave snippets of information through which one can deduce the likely situation. It seems that VHA's customer management and billing system is used by all VHA dealers to service the needs of customers, ranging from new services to billing and other enquiries, and so on. On the surface, that would seem to be OK – the same basic model applies with banks and many other forms of organization. However, VHA's model is compromised because at least some of the dealers are not VHA owned outlets. Rather they are separate companies that act as agents for VHA. Clearly, it is operationally efficient for these companies to directly access the VHA systems for new connections and so on – it would be costly and inefficient to try to operate any other way. But while it might be OK to give VHA agents access to the VHA systems to manage their customers as a subset of the overall customer base, it seems that VHA neglected to put in place the controls required to shield customer details from access by other dealers. While there might be an argument that a customer should have seamless service from any VHA dealer outlet, there would also seem to be an argument for some additional controls, as there has been at least one published case of dealer staff "surfing" the customer database in search of what we might call "business opportunities".

However bad the practice of digging through customer data might be, it pales into almost insignificance when one understands the core failure of VHA in securing customer data. Again, journalists pursuing the story have uncovered that VHA's practice for granting access to the customer system was to assign a single user identity and password to each VHA outlet. This same user identity and password combination was known to and used by all personnel in the store, and apparently was not changed frequently. This regime has several profound weaknesses, including: departed personnel still have details of access codes and passwords; and any specific access to a customer's data can only be traced to at most a single outlet, rather than to a specific individual.

Another story contains a tantalising hint that VHA also might not have limited access to its internet customer management portal to only approved outlets. It says that VHA now requires its dealers to access the system only through a single static internet address. The likelihood seems to be that previously, anybody who knew the web location of the VHA system, and had any dealer's login and password details, might have had unfettered access to data from anywhere.

Were we top coin a banking metaphor, it would be like giving all staff, at every branch, identical keys to the vault, and probably like having no back door to the branch. It would be impossible to know who had taken what from the vault, let alone what had happened next.

Can anybody argue that the information security at VHA appears, on the face of the reports, to have been inadequate? Would anybody disagree that the word "inadequate" is itself totally inadequate to describe the extent of the failure?

Now we could continue this discussion with an exploration of the technical options that VHA might have used to provide adequate security over its business data and the private and personal information of its customers. But there are plenty of others better qualified to address these matters. Instead, we will explore the governance issues.

So VHA is a company that, because of the nature of its business, stores and maintains an extensive set of private and personal data about its customers, including financial data, credit card data, and data can be used to identify business and personal activities, travel, personal contacts and so on. The company would be subject to a range of laws and regulations emanating from various sources, in fields of privacy, telecommunications and payments systems.

Clearly, as part of evaluating its information security obligations, VHA should have become fully informed about the application of these laws and regulations and the specific obligations and expectations they impose. By correlating this information with its business model, particularly its practice of interfacing with its customers through third parties, VHA should have recognised that it would be necessary to impose a very strong regime of security control that both protects customer information from inappropriate and unauthorised access, and provides a highly reliable audit trail of what actions were performed by each and every agent accessing the customer data, for any reason.

None of this understanding and awareness requires any knowledge of information security techniques and technology. Anybody who has worked in an environment subject to secure keys for doors and filing cabinets will be familiar with the basic tenets of the minimum security appropriate to VHA's customer data.

Based on the knowledge gained through the evaluation of the security obligations, VHA should have been in a position to develop appropriate policy that would then have guided:

- establishment of appropriate control technology;
- preparation of relevant clauses in dealer agreements;
- preparation of training and other employment related material for dealer and VHA personnel;
- preparation of induction and termination procedures and protocols applying to dealer and VHA personnel;
- establishment of monitoring and response mechanisms to highlight and deal with unusual or suspect behaviour;
- establishment of a channel through which individuals could confidentially report suspected breaches of policy and controls.

Still none of this requires specific knowledge of information security techniques, let alone the underlying technology. By asking questions corresponding to the above points, and obtaining verification services from experts, the executive management and board of VHA could have established with considerable certainty whether VHA's information security arrangements were adequate. Even a request for an explanation of how customer information was protected should have resulted in alarm bells ringing loudly, as it would have been abundantly clear that the existing approach was laughably inadequate.

VHA, and probably many other organizations, should benefit from applying the guidance in ISO 38500 to their information security situation. They should:

- evaluate their obligations with respect to information security;
- direct the behaviour of the organization and its personnel with regard to information security, through establishment of appropriate policy and through appropriate investment in information security arrangements;
- monitor the effectiveness and efficiency of the information security arrangements, and the conformance of the organization, its personnel, agents and other relevant personnel to the appropriate published policies.

At a minimum, the overarching policies of the organization should establish:

- how responsibility for information security is allocated across the entire organization and its associated entities;
- how information security obligations are addressed in development of the organization's business strategy and more detailed investment and operational plans;
- how every investment to acquire new or changed business capability attends to the associated obligations for information security, and how specific proposals for investment in information security are prioritised, funded and advanced;
- the performance goals for information security, together with the risk management arrangements required to ensure that the goals are consistently attained;
- the conformance regime applicable to information security, through which the organisation and its stakeholders obtain assurance that the security arrangements are effective and that unacceptable weakness and breaches are resolved;
- the necessity to understand the diverse human stakeholder communities and to craft specific elements of information security arrangements to address the behavioural characteristics of those communities.

Directors should, in the wake of the VHA experience, ask direct questions about their organization's information security obligations and arrangements.

New Opportunity to Improve

It's early days yet, but Victoria's HealthSMART initiative is in the news again, from a governance perspective. The new government appears to be evaluating the initiative, to establish whether or not it should continue.

Infonomics has been critical of HealthSMART for a long time. It has seemed to us to be an old fashioned silver-arrow initiative where well-meaning technologists attempted to drive change in the business of health care without engaging, let alone fully understanding either the business of health care or the people in the business. Sure, it has delivered a bunch of technology, but we are still wondering about the health (business) outcomes. Already in the press commentary of the questions being asked by the new minister we've seen HealthSMART likened to MYKI, the much criticised public transport ticketing system that is still to convince most pundits that it will work. We've also seen reports just today where a leading clinician confirming that HealthSMART was not designed in conjunction with clinicians.

Some are saying that, with over $300 million invested to date, it's too late to kill the program.

Infonomics suggests that there is a simple question to be addressed: *Given the current situation, and recognising that expenditure to date is unrecoverable sunk cost, what is the business case for continuing with HealthSMART in its current form, or in any revised form?*

We'll look further at HealthSMART as the story unfolds and, no doubt, again provide some free advice to the new government of Victoria.

The Infonomics Letter Delimited

Australian readers of The Infonomics Letter may have noticed an echo recently. Some of the discussion in recent editions of The Infonomics Letter has caught the attention of industry journalist Renai LeMay, and his technology news site, Delimiter. Infonomics is delighted to support Delimiter, and from time to time content from The Infonomics Letter will appear in the daily Delimiter bulletins.

Renai LeMay also contributes to ZDNet in Australia, and as a result, some of the Infonomics material published on Delimiter also appears as opinion pieces on ZDNet. This replay of our recent comments on the Reinecke report is one case in point.

Foreign Elephants

Waltzing with the Elephant continues its journey into the libraries of more and more leaders in the business and IT fields. It was a delight to ship a significant volume of books during the December Special Offer period. We're looking forward to feedback from those readers.

With growing interest in governance of IT, it's a delight to announce two important advances for Waltzing with the Elephant:

- Commencing in the next few days, Waltzing with the Elephant will be available for purchase in downloadable PDF through the UK and US websites of IT Governance Limited. The substantial presence of IT Governance limited in the international marketplace is sure to increase awareness and availability of the book and should, we hope, bring many more business and IT leaders to a more complete understanding of how they can direct and control the use of IT in their organizations.
- Spanish speaking communities around the world have shown strong interest in ISO 38500 and its messages about governance of IT. During the past year, Miguel García-Menéndez of Madrid has laboured in his spare time to translate Waltzing with the Elephant into Spanish. His project is now near completion of the translation phase and, following a thorough proofing review, we expect to publish the Spanish edition. Those who would like to receive a first-run print copy should lodge their requests early. Further details will be made available as they come to hand.

Recent/Coming Events

Thank goodness for Australia's extended Christmas / New Year / Summer holiday break. It's been a great and essential opportunity to recharge the batteries, with a clear calendar between December 3 and January 20.

Sydney, January 20: Dimension Data Learning Solutions hosted an intimate group for a briefing on governance of IT and the educational services that Infonomics will be offering during 2011.

Kuala Lumpur, 26-27 January 2011: Expitris Worldwide presents another two day class on governance of IT. This class is heavily booked, and reflects a growing level of interest in ISO 38500 across the region, and has attracted participants from as far afield as the Middle East.

Look for more events news in February as we finalise arrangements for a series of Australian and international briefings and training classes.