The Infonomics *Letter*
Plain Language about Leadership and (Corporate) Governance of Information Technology
November 2012 Edition

Digging deeper

Hello and welcome to The Infonomics Letter for November 2012.

This month is dominated by the final instalment in the extremely popular Questions for Directors series. Already, the questions are being republished with permission in other journals, and savvy specialists are using them to both explore IT as well as build stronger boardroom skills. In this final instalment, we look at eleven questions to ask about operational performance and risk associated with use of IT. As you read them, ask yourself how well your organisation fits the desired profile.

The Spanish Elephant is on sale, and personalised copies are heading out the (email) door on a regular basis. We've just filled an order for 25 licenses from a university, giving some confidence that the next generation of Spain's business leaders will be better equipped to govern that nation's use of IT.

To help speed the Spanish Elephants, and to thank all Infonomics supporters from around the world, I've decided that for the month of December, all PDF editions of Waltzing with the Elephant sold through the New Infonomics Shop will double up – an unbeatable two-for-one deal. Look for the special deal from December 1st.

We've also enjoyed a new experience this month, of providing intellectual property for use by a major consulting firm. The Infonomics ISO 38500 Assessment Diagnostic was used by an experienced consultant with no other special training and just a little support from me, to explore how his client organisation goes about directing and controlling its use of IT. Of course, the request for the review was driven by concerns about the effectiveness of the organisation's IT arrangements, and feedback indicates that use of the tool gave a very clear understanding of the issues and underlying behaviour. Of particular interest in this case was that the use of ISO 38500 was at the specific request of the client CEO, who had read the standard and considered it a useful framework in which to understand what was happening.

ISO 38500 has popped up a number of times recently. I've seen the ISO 38500 model in documentation for a new approach to governance of IT in a major Australian university, and in the draft ICT Strategy for the government of Victoria. A consultant in Queensland also reports using the standard to help frame new arrangements for governance of IT in one of his clients. Is this a sign of things to come? Where have you seen ISO 38500 being used?

Please enjoy!
Mark Toomey 29 November 2012

Double Elephant Sale

It's almost Christmas, and time to thank all those who have supported Infonomics throughout the past year.

For the full month of December, every PDF (English or Spanish) edition of Waltzing with the Elephant sold through the New Infonomics Shop will come with a free extra named license. That's two copies for the price of one.

Purchasers will simply provide two names for each purchase, and the books will be inscribed with the license for each named person. Perhaps the CIO can buy a copy for the CEO, and keep one for personal use. Maybe the CEO will buy one, and give the second to the chair of the board audit or risk committee. The consultant might buy one, and give the second to his or her client. The only restrictions here are that the special applies only to individual purchases, and not to volume orders (unless by special arrangement – to discuss, please contact Infonomics).

For more information, wait until December 1 (I have to do the setup) and then visit The Infonomics Shop.

Questions for Directors – the series

This month, we conclude the three-part series designed to equip directors with questions that they could, and should, ask about their organisation's use of information technology. The series was prompted by a participant in this year's Company Directors' Conference technology forum, who said something to the effect of: *"I am new to the role of director, and I am concerned about information technology, but I have no IT knowledge. I came to this forum hoping to learn what questions I should ask, as a director, about IT".*

In the first part, we looked at questions about strategy, framed around the contemporary realities that information technology is a key enabler to future business models and that the way other entities in the market use IT can now have a direct bearing on each organisation's own business strategy.

In October, we looked at investment in IT-enabled change, and posed questions for directors to ask about the proposal before they approve the investment, and more questions to help them find comfort in the continuing work to deliver the investment outcomes.

Feedback on the first two months of questions has been most gratifying. Two organisations are republishing them (with permission) in the Australian market. Matrix on Board, which serves a wide array of not-for-profit organisations, is progressively

republishing the questions in its blog. The Australian Institute of Chartered Accountants is republishing the articles in its IT/XBRL Special Interest Group newsletter.

But there is a big difference between spreading the word, and using it. One organisation's IT chief told me recently that his board has no understanding of IT, so he is using the questions to educate them. He uses questions from these articles to frame discussion with the board, and it seems that the board is engaging rather well in the conversation.

Would you consider telling us how you are using these Questions for Directors?

Questions for Directors – the third instalment

This set of questions focuses on operational performance and risk associated with use of IT.

It seems now to be quite well accepted that IT is an essential part of the fabric of most businesses, and the need for it to be effective and efficient should be unarguable. It's true – the rate of IT failures in operational business use is far lower than the rate of failed projects (imagine the chaos that would prevail if between 50% and 93% of all IT systems were chronically unreliable and prone to error). But operational IT systems do fail, and the consequences of failure can be immense.

When I teach the ISO 38500 Foundation Class, I discuss an array of failures from around the world, spanning back to 2004, where the common element in the failure is that they have become headline news. Half of these are operational failures.

One case we discuss there is the case of the reservations system failure at Australia's second major airline – Virgin Blue (now Virgin Australia). With no means of checking passengers onto flights, Virgin was stuck fast, unable to move the thousands of commuters and holidaymakers booked to travel that day. The cost to Virgin in the end was not all that much – they recovered the loss by suing the reservations system provider – but at the time it represented 15% of the year's profit, and resulted in a 3% drop in the company's share price.

Another case that hasn't yet made its way into the classroom discussion is that of National Australia Bank's transaction processing failure in December 2010, when transactions were not posted to customer accounts for more than a week. Again, this probably did not cause any great impact on long term profit, but it did impact many banking customers both directly (those whose transactions were not posted) and indirectly (those who received delayed payments because of the problem). It was likely to have been a key consideration for the Australian Prudential Regulatory Authority in its decision to require a higher level of reporting on IT problems experienced by banks and other entities subject to its oversight.

There are many, many more cases of operational IT failure that damages business and parts of their stakeholder communities. It's not the purpose of this article to explore them all in detail, but rather to set the scene for an assurance that, through asking well-directed questions, directors can lower the risk of negative events in operational IT use, while also maximising the value of installed IT inventory.

Do the business managers understand and accept responsibility for ongoing operational use of IT?

This is fundamental, and we can't stress it enough: Information technology is a tool of business, and those who run the business are the ones who use, and therefore have a user's responsibility, for the enabling IT systems.

It might seem strange at first to expect business managers to take responsibility for their use of IT systems, but think of other business resources and you can see we do it all the time in other contexts. The HR function does not have sole responsibility for the management of personnel, for example. Where an organisation has a vehicle fleet, we do expect the people who drive the vehicles to plan their journeys, and operate the vehicle within its performance and capacity limits, while also complying with relevant laws and regulations.

Business managers should have a clear understanding of what IT systems are required to operate their part of the business. They should understand whether those systems are fit for purpose, reliable, and capable of processing the reasonably foreseeable business peaks when they arise. They should know how long it takes to make changes, how many faults the system is running with, and how soon it will need a major overhaul.

Do the business managers understand which business activities are critically dependent on IT?

It's worth asking this question again, in its own right. Don't ask the CIO for the answer to this question, though – ask it of the business managers, and ask them to explain the dependence. Look to the CIO for validation – to confirm that the managers understand correctly.

In days gone by, when people joined companies as juniors and stayed for life, knowledge about how the business operates was an intrinsic part of the career. When things went wrong – whether in an IT system or elsewhere, people knew enough to know what to do and keep the business operating.

Now, people move frequently from job to job, flitting from one organisation to the next, taking scant time to learn the detailed workings of one business before moving on to the next. Situations can quickly develop

where nobody in the current ranks knows why a business operates in a particular way, because nobody was there when the design was put in place, and nobody since has taken the time to discover the detail.

This atrophy of corporate knowledge can be exacerbated by two aspects of IT. First, when business rules are coded into an IT system, their ownership becomes confused and ultimately lost, and soon after, the detailed knowledge of the rules fades too. Many organisations, not least of which are the Australian Customs Service and the Australian Taxation Office, have discovered that when it came time to replace the old computer systems, there was no documentation and no knowledge of the detail – they had forgotten how their business operated!

So ask the business managers which activities are critically dependent on IT, and ask them to explain the detailed nature of the dependence. It will force them to learn a great deal about the business. As they explore, they may well find opportunities to improve and streamline performance, and they may uncover risk to be managed. In some cases, they may even discover gems of capability that have fallen into disuse, which can be revived to drive new value.

In some cases, business use of IT deviates quite markedly from what is expected and understood by the IT specialists. Where systems have been operational for some years, the experiments, innovations and, sometimes, misconceptions of individuals, become "ironed on". Little pieces of user-developed IT – spreadsheets, small data bases and suchlike, become hidden keys to operation of the overall business, bridging gaps in and between systems and catering for requirements that emerged after the original system was installed. Increasingly, internet based services are used to augment established IT systems, often without knowledge of the IT function and sometimes without even the explicit knowledge of the more senior business managers. Knowledge about how to use a system and what its capabilities are becomes coloured by individual experience and perception, and through "Chinese whispers" the use of a given system can both change and become limited.

So apply an old adage: you can't manage what you can't understand; and ask managers questions to ensure that they understand how their part of the business works – so they can manage it!

How long can the business tolerate an essential system being unavailable?

It goes like a fairy tale: once upon a time, there was a business that operated manually, and then installed a computer. When the computer went wrong, as it often did, the people in the business shrugged their shoulders, and reverted to the old manual method.

Sorry – that doesn't work any more! The computer is no longer just automating what we did manually – it's enabling us to do things that we could never have done in the manual space. And even if that's not the case, the likelihood that people can remember the manual version is so close to zero that it makes no difference.

When essential IT systems fail, business stops. If they fail for too long, the business and its relationships can be severely damaged. Knowing how long your business can tolerate a failure is essential management knowledge that goes directly to conditioning the way that management works to prevent unacceptable failure from happening, and to ensuring recovery from failures that do occur in an acceptable timeframe. Which raises another point – just who defines what is acceptable? How do managers form their views on this? If they don't consult stakeholders, for example, there is a risk that their view is not what the market expects, and the market, particularly in the online world, is remarkably unforgiving of IT-enabled failure!

Who is responsible for managing the business impact of an escalating service disruption?

When an IT system fails, there's a good chance that the first people to realise will be the IT team – right? Not these days! There's a high and increasing chance that the first awareness will actually be your customers – and that means that, with social media enabling people to communicate issues almost instantly, your technical problem can rapidly escalate to a PR catastrophe. And the longer it takes to solve the problem, the more damaging can be the fallout.

When an IT system fails, you need the IT experts and probably a core group of people who deeply understand how the business works to address the challenge of fixing it. But don't expect them to also manage the bigger picture – for that you need a different set of skills – business skills. You need people who understand how the business works (yes, more of them), the expectations of the market, of the regulators, of suppliers and other stakeholders. You need people who can devise ways of containing and managing the impact of the failure before it becomes unmanageable.

Of course, all this should be part of your business continuity plan. But is it? Do your managers know what the business continuity plan requires of them? Do they know, through testing it, that the plan actually works? Do they know, through regular training and practice, how to do what the plan requires them to do? Is the plan focused only on restoring service, or does it include measures for understanding and controlling the collateral damage?

What evidence exists that the personnel responsible for operation and management of the IT systems are trained, competent and current in the procedures required to recognise a system failure, and to initiate and conduct a complete transfer to fallback?

The failure experienced at Virgin Blue started as a technical fault that, in theory, "could not happen". Industry scuttlebutt tells us that there was a procedure for failover to a standby system, but that the operator did not follow the procedure. The actions that were taken resulted in the hot copy of data on the fallback system being damaged, requiring a rebuild of the data from backup and transaction records.

When Transurban's Citylink tunnel safety system failed in early October this year, it threw the Melbourne traffic system into instant gridlock. The standby safety system did not successfully take over the task, and the travelling public had to wait hours while technicians diagnosed and corrected the cause of the fault. It's not too hard to conclude that Transurban had not done enough rigorous testing of its failure recovery procedures.

This writer once heard the tale of how the board of a major bank diligently checked that quarterly disaster recovery tests had been completed successfully. Of course the answer was always "yes". Then a director asked: "what is the definition of success"? You think it a naïve question? It wasn't! The presenter did not know, and took the question on notice to report back to the next board meeting. And at the next meeting, the presenter gave an embarrassed explanation that "A successful test is one that fully completes transfer to the fallback system, or fails to complete but the cause of the failure is established within 24 hours". In reality, the bank had been unsuccessful in its disaster recovery tests, and in breach of its license, for nine successive quarters.

Nowadays, stakeholders expect that failures should not occur, and that when failures do occur, they are resolved swiftly, completely, and with little, if any, consequential impact on the stakeholders. In most cases, this won't be possible unless people know what to do, and know enough about the business, to contain and resolve problems. Building and embedding the knowledge for managing and recovering from a technical failure is not an overnight task, and it's made more complicated by the propensity of people to move out, rather than up, requiring a more intensive focus on maintaining capability and knowledge as the people change.

At the end of the day, then, there is no substitute for real experience and evidence that the people required to manage and recover from an IT systems failure are available, competent, experienced and up-to date – and that evidence can only be derived from rigorous practice and testing.

To what extent is front-line staff knowledge of how to effectively use the IT based on hearsay, rather than formal, rigorous training?

Most IT-enabled projects (IT projects) include budget for training the people who will be hands-on users of the new IT system(s). Smarter organisations extend this budget to cover not just the use of the IT, but full job training for the new business model or capability that is enabled by the new IT. Sadly, many projects start out with good intentions, but when time and budget stress emerge, training is one of the first things to suffer.

But there is at least some chance that people who are the first users of an IT system will get *some* training. What about when they move on to other roles, and new people come into the user community? There's unlikely to be enough of them to justify mounting a formal class, let alone rolling out the full program that was used when the system was first installed. The temptation is to skip formal training and have them learn "on the job" from their supervisors and peers.

Now if this is accompanied by a formal learning management framework, such as a target knowledge specification, a reading list, online tools and, ideally, a knowledge and skill test, it may be an ideal way to educate small numbers on a continuous basis. However, such rigour costs money to establish and maintain – and who has the time for such activity nowadays?

When new users learn their jobs by hearsay – absorbing it from the people around them and through their own experimentation, they are likely to absorb a mix of correct, incorrect, prejudiced and perhaps even perverted information. What they learn is influenced by the experience and perspective of their teacher, who may also have learned hand-me-down information that is incorrect and incomplete. In worst case scenarios, major capabilities of a system can become lost, not because they have been removed, but because people do not learn how to use them, or they form incorrect views of the capability and cannot recognise its value.

A robust skill and knowledge development program is probably essential in most organisations today. Some professions require not just specific entry knowledge, but continuous professional development. What about the workers in your organisation? You may be looking for specific credentials when you hire them, but what about the gap between their external knowledge and the knowledge they will need to perform their role effectively and efficiently? And what about when people are transferred from one role to another within the organisation? Does your skills-management program equip them with accurate and sufficient knowledge of the systems they will use?

Which aspects of current business operations are suffering from inadequate IT service?

It's unlikely that business remains static over an extended period, and what was satisfactory at one point in time may not be OK at another. Think about the growing family and the family car for a moment to get the picture – the new couple may be well served by a sports coupe, but the first baby changes all that – and by the time number three arrives, a large

people mover is required to transport the entire clan, including pets and supporting equipment. The journeys made and the driving skills don't change much, but the vehicle certainly does.

Many factors can put IT service under stress. The business workload grows, but the infrastructure and sometimes the architecture of the IT systems present limits to capacity – most of which should be manageable through routine attention, as long as the rate of change is being properly monitored and managed.

The changing business environment creates a different stress for the underlying IT systems. Changing business models, regulatory environments, customer demand and many other factors drive demand for change in systems. Over time, change impinging on change carries the system further and further away from the clean design of its early days. Compromises driven by technical constraints, urgency, lack of expertise and tight budgets conspire to make systems much more complex than when they were new. Inflexibility and costliness become prime characteristics of the system. Competitors with newer, more nimble systems drive market demand and impose greater stress on your systems, forcing you to compromise further, or fall by the wayside.

Sometimes the answer to stress is to bite the financial bullet and commission an overhaul – but not always. Sometimes, it might be better to exit that part of the business – cut off the costly part and focus on the parts that work (or can be made to work) well.

It can be difficult for IT people to know the real impact of IT constraint on the business. If a system is performing within its design specification, it may be seen as not under stress. But if that same system's design specification is now far removed from the needs of the business and its stakeholders, there is a problem – the system no longer does what its business owners and users require. Whose problem is that? Unquestionably, it's the business leaders' problem – they have the job of mixing the full suite of resources to deliver the business. In the short term, business leaders might be able to offset a constrained IT system by adding more of another resource – such as people – but in the end, the constraint will have to be addressed. Who is better placed to understand the timing issues for addressing such a problem? Surely that's the business managers as well.

When a business manager explains the known stress points, there should also be a positive confirmation that other aspects of the business are not under, or likely to be under, the stress of inadequate IT service. There should be evidence that the managers are not simply reporting the things that are causing them immediate grief, but that they are taking a proactive approach to knowing the operating condition of the business and its enabling IT, and can plan ahead to take pre-emptive action before a stress becomes fatal.

What assurance do we have that all of our data is securely protected against loss, inappropriate access and unauthorised change?

Information security and protection is a hot topic today in most parts of the world. The prominent tip of the iceberg here is the concern for privacy and identity theft – and we see many cases of disclosure being reported in the press. It doesn't take much thought to realise that the sensitive data is only one part of an overall sea of data that is essential to the successful enterprise.

Think about the last commercial flight you took. What assurance was there that the pilot and co-pilot could each successfully land the plan at journey's end? Surely, one can expect that an experienced pilot can do this almost while asleep – but is it just this experience on which we rely? Absolutely not! There are layers of protocol that guard against accidental error – checklists that ensure attention to every step in the process, interlocks that prevent things being done out of sequence, and cross-checks between individuals to verify critical steps in the landing sequence. Increasingly, automation is used to lighten pilot workload, but pilots still carry the ultimate responsibility for ensuring that everything is correct, and pilots undergo continuous training that maximises their expertise for different landing conditions.

Should we apply that level of assurance to the data in our organisation? Immediately, the cost/risk radar comes into play. What is the risk of important and sensitive data being damaged, or being accessed by people (and systems) that should not access it?

In some jurisdictions, that question is being answered by legislators, who are enacting data protection legislation with draconian penalties that apply whenever data "escapes". In others, it is the "court of public opinion" that drives the balance. It's a topic about which there will be a great deal more debate, legislation, regulation and case law in coming years.

But would you really want to wait to be forced to ensure that the data on which your business operates is safe? In some markets, your data is your competitive advantage. In others, security of data is intrinsically linked to your "social license to operate" and if you lose the trust of your stakeholders, they are likely to abandon you and give their business to a competitor. Vodafone in Australia is struggling to rebuild its business after massive customer defections driven by a failure to maintain network performance that was aggravated by exposure of extraordinary weakness in information security practice resulted in serious customer privacy concerns.

Most organisations today should have clear and robust information security policies, that are deeply inculcated into all personnel and associates. There should be technical controls that enforce the more critical elements of the policy. There should be clear assignments of responsibility for all aspects of data

protection, with protocols that ensure diligent attention to those responsibilities. There may be value in a continuous education program that informs personnel of the policy and their duties, and equips them with the necessary skill to do what is required.

Maintaining backup copies of data has been a part of IT since the first storage devices were deployed. But many organisations have learned the hard way that the simple act of "running a backup" is not sufficient. Just as the airline pilot is complemented by protocols and practice, there is no substitute for relevant protocols and practice around backup – to confirm that backups are taken, to confirm that they are complete and error free, to confirm that they can be reloaded successfully, to confirm that transactions which have no originating source document (such as online purchases) are recorded in such a way that they cannot be lost, even in the most catastrophic of circumstances.

Finally – a word of warning about Cloud Computing. Some people seem to think that the cloud is operated by beneficial technicians who will cover off all of our omissions, at no cost to us! They seem to think not just that backup is integral to the service, but that it is complete and will serve their unique needs with no further effort. The reality is far harsher, as learned by hundreds of customers of Distribute.IT, an internet hosting firm which had all its servers destroyed in an extreme case of attack by hackers. Most of the data stored on the Distribute.IT servers was lost, with much of it not backed up anywhere. The Distribute.IT service did not include backup of customer data (including their websites), but many customers had not taken any other precautions.

What hard evidence exists that we can achieve timely recovery from a major loss of IT assets?

Our experience of personal technology can lead to false assumptions in this regard. When a PC fails (as was the case at Infonomics just a few weeks ago), the recovery process is straight forward – go buy a new PC, reinstall all the applications, and reload the data from backup (here, the whole exercise took about 6 hours). But even that can be viewed as slow - it takes but a few minutes to buy and install a new app on a current generation smartphone or tablet.

When we are dealing with enterprise level systems and technology though, the issues can be very different, and the work required to recover after a major loss of assets can be substantial. While few organisations can justify a complete real-life exercise to assess a reconstruction, there should be reasonably developed plans that can be independently assessed, showing what has to be done, where the critical decisions must be made (and who makes them) and how long the main steps will take to complete.

It's important for the plan to consider all of the IT assets and how they can be recovered or replaced – as some may be constrained by matters such as supply and others by licensing and ownership. It may be OK to have a plan say that to replace a single PC, we simply go to the corner PC store. But what about if your systems are locked in to an otherwise obsolete technology that can no longer be readily sourced? Some plans will require prudent arrangements that assure availability of key assets in case of a disaster.

Preparing a plan for recovery is one thing. Keeping it up to date is entirely another. The IT asset in most organisations is constantly changing and recovery that enables business survival after a major loss of IT assets will require reinstatement of current capability, not the capability of the organisation at a snapshot point that may be three or more years old. Some organisations may find it useful to impose a protocol that requires a refresh of the plan annually, or even more frequently.

Finally, a recent incident in the regional town of Warrnambool, on the southern coast of Australia, serves to remind us that we are dependent not only on our IT assets, but those of other organisations. Fire destroyed the main telephone exchange and cut around 60,000 landline, mobile and internet services. While news reports show that Telstra, the major telco that owns the exchange, has a highly developed plan for service restoration, including rapid deployment of temporary mobile exchanges and a cascading priority list of services to reinstate, many businesses had no contingency plans and were operating on the assumption that the basic communications service would continue uninterrupted, forever.

Do we have the capacity and knowledge to analyse and recover from a serious fault in our key IT systems?

When our car breaks down, we take it to a specialist who has the training and tools to diagnose the problem and affect a repair. Part of that specialist's core training involves building a sound understanding of how a car works, and how to test the various systems and, increasingly, detailed knowledge of specific models of car.

When Richard Champion de Crespigny and his crew experienced a catastrophic failure of an engine in an Airbus A380 flying out of Singapore, he drew on his more than thirty years' experience in military and commercial aviation, and his in-depth knowledge of the aircraft he was flying, to first stabilise what was in reality a mortally wounded aeroplane, and then land it safely (if not without considerable drama – De Crespigny's book, QF32 is an enthralling read that contains real lessons which can be applied far wider than just in commercial aviation), at Changi Airport.

The information systems that enable most modern business are often, and necessarily, extraordinarily complex. The overall IT system for an organisation is probably an eclectic mix of purchased product and custom setup, developed over a span of several (if not many) years, probably sourced from several

providers who operated with different standards and disciplines. Knowledge of what the systems do, of how they work, and how to fix them when they go wrong is essential. Assuming that they won't go wrong, or that if they do go wrong "somebody" will have the answer, is an act bordering on negligence.

Just as we see with the car and the aeroplane, dealing with a problem in an organisation's IT requires a sound and comprehensive appreciation of the IT systems and how they fit into and serve the business. While documentation is an essential element of the organisation's ability to diagnose and resolve problems, it does no good if there are no people who have the expertise and local knowledge to use the documentation.

Most of the time, we should avoid having heroes looking after our IT, but there are times when it is highly desirable that somebody, or preferably several people, can deliver in a heroic fashion – simply because somebody dared to ask if we have the capacity and knowledge to analyse and recover from a serious fault in our key IT systems.

What aspects of our business activity, our future business performance and our obligations regarding protection of data are at risk due to uncontrolled use of external IT services?

As few as ten years ago, this question may have been irrelevant for most organisations. How quickly the world of technology-enabled business changes. The growth of the Internet has spawned a new phenomenon we call cloud computing – in which data storage and business functionality can be purchased and used from any device that has access to the internet.

For many in business roles, cloud computing has been the answer to a long-standing prayer for release from the perceived restrictive practices of the formal IT department. But where some aspects of this release have been used appropriately, there are many cases where it has been used inappropriately – and often with full approval of senior managers who have not understood the risks.

Using external IT services, whether in the cloud, or through an outsourcing arrangement, carries risk, and that risk should be properly understood by all who are making sourcing decisions. Where once sourcing decisions were quite major, and limited to the executive team and the board, credit card access now gives sourcing decisions right to the coalface in many organisations, and without control, the risks are hardly likely to be identified, let alone properly controlled.

The unceasing growth in capability of technology serves as both a blessing and a curse for organisations. For example, technology enables an organisation to operate as a much more integrated whole – presenting itself to customers, regulators and other stakeholders as a seamless, smoothly operating unit. The blessing becomes a curse when those same entities, having seen the advantages of a seamless organisation, expect that seamlessness to be perfect, and to exist across all organisations. But seamlessness depends on a substantial harmony between the many IT and non-IT systems through which the organisation operates. Uncontrolled and imprudent use of externally sourced systems can disrupt that harmony and cause at least inconvenience, if not damage, to the systems, and introduce the risk that necessary controls are not applied to all of the IT resources used by the enterprise. A recent case in point in this regard has been a requirement by Singapore's banking regulator that a bank desist from use of Salesforce.com, due apparently to insufficient confidence in respect of data security and jurisdictional reach.

None of this discussion is intended to say that organisations should not use external IT services. Rather, it says that organisations should be as aware of the external services they use as they are of the internal services, and that they should understand the implications of each case. It probably also means that they should establish clear and rational policies that enable the organisation to perform competitively in its market while containing the risk. There should be guidelines for decisions about use of external IT, coupled with education for the people who may find themselves contemplating such a move.

Finally, organisations should consider the specific case of external IT that is actually owned by the individual employees. Already, it has become clear that absolute prohibition of such use is impractical and often counterproductive. It's probably far more important to manage the reality, to understand the risks, and put in place the means by which employee-owned equipment is as safe to use as that owned and controlled by the company.

So there we have it – another eleven questions for directors to ask of their executives, or for executives to ask of their managers, and so on. How will you use these questions? Can you answer them all to the extent that you would be satisfied with your own answers? What will your peers and colleagues do if you put these questions to them? Can you follow the lead of the IT Chief I mentioned earlier, and use them as a tool to help increase the capability of your executive managers and directors to probe the IT situation in your organisation, and others?

Perhaps your answers to the questions are unsettling. If they are, why not ask for help, or have a closer look at Waltzing with the Elephant to learn more about how your organisation can effectively govern its use of IT?

And as we count down to the next edition, stay safe, and enjoy life!