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

Close to home

Hello, and welcome to the March 2010 edition of The Infonomics Letter (yes, I know – a tad late again!). This one comes from Auckland, New Zealand, where I have been the guest of Brightstar Conferences at their annual IT Governance, Audit & Information Security Summit. As always, conferences allow me to not just share my thoughts on governance of IT, but also to learn more about what others think. It's clear that more and more people in the IT supply space are understanding that governance is different from management and that there is a major demand side weakness to resolve. Some of the significant challenges for these people revolve around getting engagement with the business leaders. For many, my advice is to strive to put the discussion squarely in business terms, focusing on business issues and consequences, and using analogies that will be familiar to the business leaders. I describe IT as merely a tool of business, and in that regard it is not unlike buildings and plant – physical elements that business leaders have no trouble understanding.

Another way of dealing with the communication issue is to describe the governance scenario in terms of somewhat simpler constructs. I had been thinking about doing this in terms of governing IT use in the home when Microsoft delivered results of its research which shows that parents don't do enough to direct and control the use of IT in the home. Unsurprisingly that cemented that plan, so this month we look at how to apply the principles for governance of IT in a domestic situation.

The conference in Auckland provided an opportunity to discuss with one of New Zealand's Assistant Commissioners for Privacy, the issues surrounding use of social networking and other internet tools. This took us to one of my pet peeves, and prompted "Keep my secrets secret, please", on the bad habits of web systems when we register as users.

Tremendous value is coming from the Infonomics Governance and Management of Information Technology International Survey which has now closed. While analysis will take some time, early results are indicating some very powerful trends and key messages. There is no doubt that there is a great deal of improvement to be wrought in what is generally seen as a vital discipline. A summary of key results should be available in the next edition.

Waltzing with the Elephant keeps rolling out the door, to all corners of the planet. Have you recommended it to your business leaders and colleagues yet?

Kind regards,
Mark Toomey

1 April 2010

Governance of IT at Home

According to a recently published Microsoft study, 65 per cent of parents do not take precautions when their children are logged on to the Internet. And 60 per cent admitted allowing their children online without any supervision or restrictions. Although 60 per cent of parents know that parental controls can be enabled, only 20 per cent have used them. Yet more than 30 per cent know that their children have downloaded illegally, and 12 per cent know that their children have disclosed personal information (presumably in an unsafe manner).

While these finds are not at all surprising, they are disturbing, and they do point to an interesting governance problem – one that can be discussed and perhaps greatly reduced by use of ISO 38500.

Consider the home environment as an organisation – a group of people who have come together for a common purpose. While it's true that some children may not wish to be part of the organisation, that is for the purpose of this discussion, a side issue. And while some home environments are comprised entirely of adults, we can probably get the most from this discussion by focusing on the classical family model – two parents and children in pre-teenage and teenage stages of development. Hopefully, most readers can extrapolate this context to their own situation.

ISO 38500 says that the directors should evaluate, direct and monitor the use of information technology in the organisation – the household. So who are the directors, what exactly do they evaluate, direct and monitor, and how do they go about those tasks?

Fairly clearly, the directors are the parents – or one parent acting on behalf of both – or those who would be regarded as the senior decision-making members of the household. Evaluating the use of IT in the household essentially means comparing the potential use of IT, including the Internet and all the things that come with it, against the current use and the needs of the family, and reaching some fundamental conclusions about whether or not the status-quo should change. Tens of millions of parents throughout the world have unconsciously made such decisions in the past ten years as they have considered the increasing availability of the Internet, and decided to go online.

But evaluating means more than being vaguely aware of what technology is available. It includes knowing and understanding the potential advantages and disadvantages of the technology, taking into account the skills and maturity of those who will use it and the actual needs of each individual. Children in primary school, for example, can find much on the Internet that is of interest and value to them, while younger

and older teenagers also have their relatively closed fields of interest. Adults may have other interests again. Some features go across the board. The needs and opportunities for each should be considered. For every advantage that is offered by the Internet there is a counterpart – a disadvantage. There are opportunities for bad behaviour, for illegal behaviour, for becoming a victim of some other person's bad behaviour and illegality, for becoming addicted, for creating serious financial difficulties and so on. This is not to say that parents should avoid connecting to the internet at all costs – rather that they should be making informed decisions.

Having evaluated and understood the pros and cons of technology in the domestic environment, the parents should then decide exactly what use of technology they will permit and if required put this into practice by making investments (buying computers, software and services) and establishing rules. Now exactly what rules are required? For this, we can take strong guidance from the principles in ISO 38500. But first, we close the governance loop – monitoring.

It is human nature for people, and particularly children, to test the boundaries and push the limits of constraints imposed on them. If they push and find no resistance, they will not generally stand back and conclude that the rules are good and should be observed even though they are not enforced. Rather they will move into and dominate the space they have found by pushing the limit and then they will push further. It's not surprising that many children have found themselves in deep uncharted territory and have fallen victim to the undesirable elements that prowl in this space.

So monitoring in the family environment is essential and, however hard it is to perform, it is an essential part of governance that protects the family from harm in numerous dimensions. And while some monitoring can be done by use of automatic tools that actively enforce boundaries or raise strong alarms when the boundaries are breached, it is likely that much of the monitoring of family use of information technology must be done the old-fashioned way – by looking over the shoulder, and engaging in conversation about what has been happening.

The principles in ISO 38500 provide a very useful framework for setting the rules, or policies that apply in a household use of information technology context. Start with the Responsibility principle – who is responsible for what, and what is the responsibility of each person in the household?

Clearly, the senior members of the household carry the major responsibility for decisions about how much information technology and how much internet access is to be available in the home, and to whom. The senior members – most likely the parents, set the rules that must be followed, clearly marking the boundaries that are not negotiable and those that can be expanded in a controlled manner when there is a suitable justification.

In order to make these decisions, it is essential that parents inform themselves of risks and opportunities inherent in the use of information technology at home. This task of becoming informed is a key part of the responsibility – it's not just about making the rules – it's about doing so in an informed manner.

We can extend the discussion of responsibility in two directions. On the upstream end, with home level information technology now regarded as an essential utility, the demand for parents to be properly informed creates a responsibility for industry, community and government to provide relevant information to parents in a way that they can comprehend, so that they can make appropriate decisions. In parallel, there is an emerging responsibility for industry that develops information technology for home use to provide parents with tools that they can easily understand and use, to help them in the often-difficult job of keeping control over children who by their very nature are always attempting to break out of the constraints.

Some responsibility also transfers to the children and others in the household. They must conduct themselves, and use the information technology in appropriate ways, so that they are able to do what is important, without undue risk to themselves and the activities for which they use the information technology. Essentially, they must follow the rules.

As is explained in Waltzing with the Elephant, the full depth of the responsibility principle can only be appreciated in the context of the other five principles in ISO 38500. Thus, this discussion of governing home use of information technology needs to also explore those principles.

The strategy, or planning principle comes next. It seeks that IT is planned to best suit the needs of the organisation. So, home IT use should suit the needs of the household. The plan depends greatly on circumstances. How many people need what sort of information technology, and at what times? Is the work that they do lightly or heavily dependent on the internet? Will the work they do be stored at home or in a remote location? Is privacy an important factor, and if so, for what? These questions might seem more appropriate to a workplace – but consider that a household with a university student, another in the latter years of high school, and one youngster. The older students will probably need a great deal of time to use the IT, since it has become ubiquitous in student life. That may drive a demand for two independent computers. The needs of the young child may be met by the older siblings sharing, but reality is more likely to be a demand that the parents have a third computer which is shared with the young child.

Many more elements must be considered under the strategy principle. What software is required, and where will it be installed? What is the real demand likely to be for internet bandwidth and download capacity? Will that be driven by social activity or by serious work? Where will computers be located? Should there be a home network, and if so, should it be done with wires or wireless? Should provision be made for ad hoc guests to use the network and access the internet? The list of questions is not infinite – but it may well be quite long. Should somebody take on the responsibility for preparing a topic list as part of a guide for parents to help them make appropriate decisions?

Responsibility overlaps strategy. While the strategy principle says that plans should fit needs, it does not specify who makes the plans. It should be intuitively obvious that for home IT, the parents should have responsibility for the major plans – though they would do well to involve the children in preparing them.

After strategy comes acquisition – the decisions about actually spending money. Well actually, that's just the start – for once acquired, in a home internet use context, there are a number of other acquisition elements to consider. Purchasing a new computer may be a significant capital event for the parents – but a minor blip on a continuing series of minor bankruptcies for a spendthrift teenager. But again, it's not just about purchasing the appliances (which is after all what a PC has become). Rather, it's about making sure that what has been acquired does the right job in the right way and that everything works together in some sort of reasonable harmony. And it's about properly understanding genuine need, separating this from fad, and making informed choices regarding the calibre of equipment purchased taking into account price and other market trends.

Who is responsible for acquisition? That can be interesting in households where several individuals have independent purchasing power. The key issues move from whether or not to purchase, to whether or not the equipment fits the rest of the home environment. Is it compatible with the equipment already in place – and does it need to be compatible? Will it displace something that is already in use, and if so, what should happen with that now obsolete equipment? Thus, even in the home context, responsibility is not merely about who has budget, but also about whether the proposed purchase fits the bigger picture.

Step now into the performance principle. It's about ensuring that the IT (as used in the home) performs well, whenever required. That's a big topic – because it is not merely about how powerful are the end computers – but also about understanding the risks that could come back to haunt.

Probably the most important subject under performance is the oft-forgotten topic of protecting data from loss – good old fashioned backup. It's a topic that many home users of IT have never had to address because pre-computer, it was relatively difficult to lose data. Certainly, books could be lost, stolen or destroyed – but that was a comparatively infrequent situation. Before home computers, there really weren't too many cases of bookcases simply disintegrating destroying all they contain, or of desks clamping themselves closed, never again to release their content. Sadly, computer storage can do the equivalent of both these things, without warning, and unlike lightning, these disasters can strike in the same place, multiple times. So it should not be surprising that one of the essential issues for good governance of IT in the home context is making sure that all the data – photographs, homework, letters, emails, contacts and so on are properly protected against loss and damage.

There are also questions of capacity that must be considered in the home environment. We mentioned earlier the one regarding how many and what type of computers are required – a result that will vary depending on the activities that each individual wants or needs to participate in. This desire, or demand, must be moderated against the relative cost, not just of equipment, but in space and time. Internet links require special consideration – how much demand will be made, by whom, for what purposes, and when. Selecting an Internet link is not merely a case of finding the lowest price for the highest advertised speed, despite the tendency of marketing material to focus on these elements. There are many ways that providers can configure services that give different levels of consistency of responsiveness and throughput – and a little research and understanding can result in quite different outcomes. And the ongoing use of internet services may need to be monitored, as there can in some jurisdictions be significant financial penalties for exceeding defined usage thresholds.

Teenagers in particular seem to have a propensity for fearlessly exploring cyberspace and for downloading all manner of digital data – some of which can be extremely harmful to machines and to persons. In the home environment it can be essential that appropriate tools and controls are exploited to help contain such exploits and limit the potential for danger. It is essential that the parents actually discover what tools and controls are available for them to use, and for them to be applied as necessary. Of course, while parents have this responsibility, it is also a clear responsibility of software developers and other providers to ensure that these tools and controls are accessible to and usable by the great majority of parents, noting that most will not have any technical expertise on which to base their decisions or actions.

Going hand in hand with performance is the Conformance Principle. This one deals with the law, and most importantly with the "home rules". Some of

the important laws that apply to information technology in the home have been discussed widely – those relating to software licensing, copyright, spam and the sending of threats. It is the responsibility of the parents to understand which laws apply, and to ensure that all of their children both understand and comply with these laws. It may also be appropriate here to remind government agencies that they have a responsibility to help parents be aware of, and to communicate the core messages in the relevant laws.

Home rules are the ones that the parents, or the entire domestic unit, decide should apply to ensure balance of enjoyment, achievement and risk in the family's use of IT. There can be many topics for home rules – but it should also be clear that a few simple rules are most likely to work best. These rules might relate to time and duration of use, priority of school work over games and social networking, sharing of equipment and resources, maintaining separate logins for each person and so on. Where there are budding computer scientists involved, the rules might also deal with keeping fingers out of key machines, rights to make changes to settings, and who gets to help when something goes wrong.

Human Behaviour – the final principle in ISO 38500, is rarely manifest as clearly as in a home and family context. Children are, generally, made for breaking rules. Therefore, there must be an appropriate level of direct monitoring. Most likely, there will need to be arrangements for consequences when inappropriate behaviour is detected. Because many children are naive, and because cyberspace can unfortunately harbour many who would exploit such naivety, there needs to be ongoing dialogue between the adults and the children to keep track of what is happening, to build understanding of the dangers, and to resolve any unwise actions that may have occurred.

This discussion has explored the applicability of ISO 38500 to governance of IT used in the home. The standard was deliberately devised to apply to all organisations. While it does not explicitly refer to home use, it should be very clear from the above discussion that it does indeed work in this context. The discussion highlights that while the standard does not prescribe specific actions, it provides the framework for thoughtful investigation and discussion of what is required to direct and control the use of information technology in a wide variety of circumstances.

This discussion has perhaps also highlighted the opportunity for development of a specific guide to governance of IT in the home context, based on ISO 38500. Such a guide might expand beyond the responsibilities of parents, teenagers and children, by exploring the responsibilities of information technology providers and regulatory agencies to provide significant support for parents who will never have any significant understanding of the technology their children will exploit with gay abandon!

Keep my secrets secret, please?

Most of us who use the Internet will have experienced the requirement imposed by many website operators to register as a user of the website, in order to access the resources and functions it provides. Some of these websites collect personal information as part of the process. Mostly, they protect the confidentiality of our private information and the settings we have selected for our use of the website, by the classical approach of a username and password combination to establish and confirm our identity.

Now the whole idea of a password is that it should be a secret known only to the individual who set it up. Website operators should use encryption tools to ensure that passwords cannot be easily discovered. To deal with the situation where individuals have lost their password, website operators should use a range of techniques to provide reminders or to provide reasonably secure delivery of replacement passwords.

But some website operators seem to have absolutely no regard for the privacy of their customers at all. These operators are the ones who, immediately you have set up your password, send you a confirming email. On the surface, this might seem to be a useful courtesy. But if you think about it, the more appropriate description might be criminal stupidity.

Standard emails are transmitted in a format that can be and frequently is easily recorded and read at several points along the journey between the originator and the recipient. With no security controls at all, these email copies can be read by unscrupulous individuals who may have no compunctions about immediately stealing your identity, logging onto the service you have just set up, and exploiting it to perpetrate further misdeeds.

It's time that we stamped out this practice. There are well proven, low cost and secure methods of resolving problems with lost passwords, which all website operators should use. The bad practices create risk to individuals through privacy violation and identity theft risk, and as a consequence, website operators are also at risk. A combination of education and enforcement is probably required. Perhaps we also need a resource where we can name and shame those lazy and uncaring operators who persist in exposing our secrets to the world.

Infonomics encourages privacy organisations all over the world to think about and act upon these issues, in the interests of creating a safer internet for all.

Waltzing with the Elephant

Have you joined the throng of enthusiastic readers? Read the reviews, then post your own on the LinkedIn Group.