



## **Information Risk Management** **Wednesday 7 July 2010, KPMG, Leeds**

This session proved very popular as the risks we face in our day-to-day use of IT are considerable and for most of us quite obscure. Indeed, risks to the confidentiality, integrity and availability of the information we all depend on to do business have never been as prominent as they are today. Information assurance and security are no longer the sole province of the IT department; information risks can have enormous financial, regulatory and reputational impacts.<sup>1</sup>

Our expert speakers were able to give us an insight into this 'mysterious' field. As ever we are very grateful to our speakers. They provide their services for nothing and often go to considerable trouble on behalf of our audiences. We owe them a great debt.

The meeting took place at KPMG's offices across the Pennines and one of the reasons for the good attendance was the many colleagues from the 'Dark Side' (the North East / Yorkshire) who turned up. We are very grateful to KPMG for making the room available and providing lunch and refreshments. Our sponsors, too, make a terrific contribution to ensuring the group survives and puts on events for our members.

Finally the meeting was organised and chaired by Ray Butler in his final fling as a North West Committee member. Ray has played a huge role in the group's success and he will be much missed. The audience showed their clear appreciation of his efforts over the 7 years since the group's inception.

Some of the presentation slides and workshop feedback are on the website alongside this note which provides a brief summary (with the responsibility for any errors or misinterpretations being mine alone!). We are sorry we cannot put them all up on this occasion, but this serves to underline the importance and sensitivity of some of the things said.

First up was Bill Hartley from Barclays PLC who talked about applying ISO 27001, the standard for information security management systems. Bill was unsure about the benefits of this, both real and perceived. It was clear that considerable time, effort and expense is required to implement the standard and yet it still does not provide comprehensive coverage. It is somewhat inflexible, yet cannot be used in isolation. On the plus side it is certainly a good place to start and provides a common framework. Bill noted that certification has more value in a business-to-business environment compared with retail where the customers focus more on *Which?* reviews. In response to a question, Bill said that senior management gave the standard their attention because of their concern about fraud levels. Other managers give it lower priority.

---

<sup>1</sup> And far-reaching ones - written on the day when TUI/Thomson's finance director had to resign because poor systems overstated sales by the odd £100m or so.



Following this, Jamie Travis summarised the latest research published in KPMG's data loss barometer, which is based on recording data loss incidents. The highest number of incidents apparently occurs in the Government/healthcare sector, though Jamie cautioned us that this is also the sector most likely to report fully. It seems clear that insiders pose the greatest threat to data security. Jamie's talk, and the subsequent question session, put considerable emphasis on the risks associated with 'the cloud', i.e. storing information on the internet with third party providers. Whilst there are many protections available, it was Jamie's view that you simply shouldn't put sensitive information on the cloud. Finally, Jamie pointed out that there are many tools available to identify vulnerabilities whether on individual computers, the network or storage. KPMG's data loss barometer can be found at [www.datalossbarometer.com](http://www.datalossbarometer.com).

After lunch Steve Rimell, an independent consultant, gave us a very spirited and clear overview of current issues in IT security. The list included: patching, SQL injection, abuse of access rights, default credentials, physical loss of data or equipment, phishing, denial of service, virtualisation (ease of creating malicious virtual machines), all the cloud risks covered by previously by Jamie, and Google hacking. You can look at Steve's presentation on the website for more about these esoteric threats and how to counter them. But the main lesson was perhaps to be sure about the security of your network perimeter (and, of course, education, education, education - the watchwords of the IRM).

The last presentation was by Steven Babb from the IT Governance Institute who put the spotlight on ISACA's new framework for managing IT risks: Risk-IT. This was produced as a response to perceived shortcomings in COBIT - no risk management process - and ISO 31000 - not specific to IT. In fact ISACA's view is that Risk-IT, together with COBIT and Val-IT (for investment portfolios) provides a comprehensive IT governance resource. More details and links are available from the presentation, which is on the website alongside this note. Guiding principles for the development of Risk-IT were: links to enterprise objectives, balancing of costs and benefits (a welcome development after the previous talks that had tended to focus on expensive 'best practice'), aligning with business risk management, open communications, tone set from the top and continuous improvement. At this point the weary reader will ask whether this is really necessary or whether wheels are being reinvented with an IT badge. This is exactly what our audience wanted know. Steve provided a robust defence of ISACA's work, highlighting the need for risk management principles to be made as accessible and relevant as possible to the IT community

The meeting was summarised concisely by Ray Butler (who was also stalwart in dealing with the unusually, and ironically, high level of IT panics during the day). Everyone could understand at first hand the value of Ray's contribution and the impact he had had over the years. We wish him all the best in his new role.

Andy Garlick  
IRM North West  
21 October 2010