GRAS Newsletter 51

October 2012

Don't Leave IT to the Experts

Summary
The topic of Information Security ("IS") is the domain of a select group of experts. Given the nature and the complexity of the subject matter, this is unavoidable to some degree. At the same time, sound risk management principles require the business to take responsibility and to be in control. That implies that even arcane areas of knowledge cannot simply be outsourced to a group of boffins without the business understanding what they do. At the very least, line management must understand what risks threaten their business and how those risks are being managed. A good starting point is to focus on the seven killer issues for your IS department.

Dear reader,
Risk management is a core competence for banks, not a luxury or an add-on. In that light, it is odd that banks should run separate risk management divisions, as if it were something distinct from the rest of the bank. The textbook answer to this is that although risk management is ubiquitous, the risk management division exists to set standards, to carry out all manner of analysis and to report findings to the senior management, thus acting as a centre of expertise ensuring some level of independence. So far so good. But there is a danger that risk management is perceived as 'something for the experts' beyond the ken, or even the responsibility, of ordinary bankers. An extreme illustration of this is the area of Information Security. IS is not a trivial problem for banks but it is rarely considered by non-experts. This, however, is a risk in itself, and although the subject matter is indeed complex, there is a simple way to bring it within the grasp of non-experts and general line management.

What line managers should ask their IS staff
The best way to bring obscure risks to the general manager's inbox is by expressing the risks in everyday language and letting the experts deal with the translation. On the topic of IS, there are seven killer issues[1] business managers should discuss with their IT security staff. These issues are relevant for any business process, but they are especially relevant for those areas that rely on IT for product development, client data handling, service delivery – which today means all banking processes. Here are fifteen questions to get the discussion going:

Issue	Background	Questions
Ignorance	Every IT solution makes use of services and parts from diverse sources. IS must ensure that no component 'flies under the radar' and thus exposes the bank to threats regarding data integrity, availability or confidentiality."	1. Do we know what the material components of our IT solutions are? 2. Do we know who the suppliers of these material components are? 3. How does IS ensure each such supplier is treated as we would any external supplier.

[1] The list of killer issues and the IS questions are adapted from an article on the seven deadly sins as described in the Information Security Forum's press release on Cloud Computing. It can be found at: https://www.securityforum.org/userfiles/public/Cloud%20Computing_Press%20release.pdf

Don't Leave IT to the Experts

Issue	Background	Questions
Ambiguity	It is essential that IT contracts are agreed with the proper authorisation and a thorough review of security requirements. Failing to do so is a major cause for unacceptably high levels of vulnerability.	4. Do all contracts follow the same form and rigour in terms of IS? 5. Are all parties subject to a formal risk assessment? 6. Do all contracts contain an IS section that is signed off?
Doubt	There is often no right to audit the service provider to establish full proof of its ability to provide the appropriate level of information security.	7. Does IS know which information security architecture, model, testing, and certifications are in use? 8. Does IS know what audits are performed at the supplier?
Transgression	Especially with outsourcing and cloud computing, legal restrictions on data handling can unwittingly be broken. Storing data in unknown locations or organisations may be in breach of privacy legislation and/or compliance rules.	9. Has IS defined approved storage locations? 10. Has IS arranged adequate controls to protect data in line with privacy legislation and compliance rules?
Disorder	When data is stored on third parties' systems, formalised access control procedures are often lacking. It then becomes difficult (or impossible) to identify and prove what third parties users can do with the data.	11. How does IS ensure that data *remains* properly classified and restricted, even when it is moved to a third party? 12. How is data access control monitored in that case?
Conceit	IT novelties must be reflected in the corporate security architecture. It is not uncommon to find banks have an unduly high opinion of their ability to protect data.	13. How does IS ensure that new services comply with standard security features such as encryption, identity and access management?
Complacency	Overreliance on a single network (such as the Internet) puts critical services at risk, especially if the service provider lacks business continuity or disaster recovery plans.	14. Is there an up to date inventory of single points of failure? 15. Are all suppliers of IT services part of the IS remit regarding business continuity and disaster recovery plans?

Conclusion

One cannot be truly responsible for risks one doesn't understand. For some topics, management may struggle to fully comprehend the risks and the controls. But focusing on the seven killer issues enables any manager to at least take part in the discussion. If your IS department enables you to answer these questions to your satisfaction, you will not be an expert, but you will be in control.