Information Security Now - 7

John Mitchell

IT Governance is a sub-set of Corporate Governance. Corporate Governance is usually defined as the *leadership, organizational structures and processes that ensure that the enterprise sustains and extends its strategies and objectives.* IT Governance may therefore be defined as a *structure of relationships and processes to direct and control the IT function in order to achieve the enterprise's goals by supporting and extending the enterprise's strategies and objectives*. Basically, it is about how the IT department is structured, lead and managed in order to help the business meet its goals in a cost effective manner.

Information security governance is a sub-set of IT governance and should therefore have a relationship with business objectives and IT objectives. The table below[1] shows the key elements of IT governance. You will notice that 'ensure systems security' sits in the 'deliver & support' domain, but the point of this table is to show that it does not sit in isolation. To achieve security at the delivery stage you need an appropriate organisational structure, suitably trained (and perhaps qualified[2]) staff, an adequate design mechanism and a monitoring process. This table is valuable to assurance providers because it enables us to identify the key inputs and outputs of the IS security process. This in turn enables us to create a holistic security assurance programme which can then be broken down into a detailed assurance process. Our detailed processes will be based around risk and controls. So the single risk of 'unauthorised access' will have a number of root causes ranging from unauthorised access by authorised staff to unauthorised access via external hacking. For each of these root causes we will expect to find fairly standard controls in place to either prevent, or detect, the unauthorised access. We will also expect to see post-event controls such as how will the enterprise deal with the media and what management trails are available to determine how the breach occurred?

Winston Churchill once said 'give us the tools and we will finish the job'. It's pretty much that way with IS assurance. We have the tools to deconstruct any IT process (regardless of the technology), identify the risks that need to be managed and then suggest the controls to manage those risks. We also have the appropriate professional qualification[3] to support out views and a pretty extensive research base to identify new challenges before they become in common use. We also make expensive use of international standards such as ISO 27799, ISO 20001, ISO 9126 and ISO 9001 as benchmarks against an enterprise's IS security. We are still surprised however, to find Chief Security Officers (CSOs) who disregard these standards.

One service provider grandly informed me that it was something he expected his subcontractors to have, but it was not relevant to the IS service he was providing to his customers. When I enquired what he had that was better than the standard, he airily informed me that his (non-existent) processes were

[1] © Information Systems Audit & Control Association (ISACA)
[2] CISSP or CISM
[3] Certified Information Systems Auditor (CISA)

superior to the standard. 'Oh, yeah', tends to be our response to such arrogant drivel. When I enquired about his professional qualification to be a CSO he mentioned a BSc in computer science. When I pointed out that his BSc was an academic and not a professional qualification he was not at all put out. What about the BCS, I enquired? Totally irrelevant was the response. It's full of flatuant academics who have no real idea about business computing. A dinosaur in a modern age? Perhaps, but was only 27 years young!

So there we have it. CSOs who are not professionally qualified being advised by assurance providers who are and who are being disregarded because we belong to a Chartered body. It's a sad reflection on life that we are often told to 'get a life' when we point out potential security weaknesses. Yes John, but it hasn't happened previously is usually the response. In that case perhaps you are due one! Remember Nationwide, HMRC and the myriad of other recent security failures. I suspect that their CSOs said the same thing to their assurance providers too.

John is editor of BCS IRMA's award winning *Journal* and Managing Director of LHS Business Control, a corporate governance consultancy that he founded in 1988. He can be contacted at: john@lhscontrol.com, www.lhscontrol.com, or +44 (0)1707 851454.