



IDENTITY & ACCESS MANAGEMENT

Executive Briefing Paper

IT Security Truths – Part 1.

This paper is a light-hearted look at some of the 'unspoken' truths that impact an organisation's ability to meet its IT security objectives. Company executives might want to delve deeper into how their organisations address these.

1. Users always take short cuts.
2. No-one takes compliance seriously, unless they are regulated.
3. Governance is reactive, when it should be proactive.
4. Good solutions cost money or, put another way, cheap security is not good and good security is not cheap.
5. ROI on security is almost intangible according to many analysts but there is no reason why ROI cannot be made tangible.
6. Open standards are open to interpretation.
7. Functionality has priority over security.
8. Information Security is viewed by non-IT security people as a 'black art'.
9. Information Security is made more complex than it should be.
10. We are better than we were but not yet good enough.

When IT security fails, it fails for one or more of the reasons above. When commissioning a new system, these truths should be addressed in the requirements and shown in the system architecture. Existing systems may require different approaches to overcome weaknesses. Organisations are unlikely to get to a zero risk position but they should be in a position where the risk is manageable.

Author:
John McIntosh
Lakebridge Limited
2010