Information Security Now - 21

John Mitchell

Rather like Asimov's three laws of robotics the information security specialist has "confidentiality, integrity, availability and compliance". Confidentiality is all about ensuring that only those people who should have access have so and compliance relates to the need to meet the associated regulatory framework. So losing data is likely to break the first and fourth rules of security. However, as the data is usually copied it is not "lost" in the accepted sense, but rather distributed to a wider audience than intended with the original owner non-the-wiser to the breach until something else happens. This may be a whistle blower, blackmail, or the use of the data for another purpose which then puts it, either accidently (emailed to the wrong person) or deliberately (wiki-leaks) into the public domain. In the UK there is a statutory responsibility to report breaches to the Information Commissioner and a search of the ICO's web site revealed that in the period from November 2007 to May 2010 1,000 breaches were reported. Since April 2010 the ICO can order organisations to pay up to £500,000 as a penalty for serious breaches of the Data Protection Act. Research by Gordon & Loeb[1] indicates that a small increase in security expenditure provides an exponential gain in the level of security. So security officers should be able to justify such expenditure with a risk analysis of the consequences of data loss, with a half million pounds fine being one of them. However, in my experience the so called controls which are meant to reduce either the likelihood, or consequence do no such thing and even where they do they usually only relate to the risks being managed by the CIO. Once the data is transferred to the end-user, then most of the controls implemented by the CIO's office become redundant. Research by a major European bank (which must remain anonymous) showed that two-thirds of IT expenditure was outside of the CIO's domain and therefore effectively outside the control of the CSO (who usually reports to the CIO). So it is not too surprising that many data losses are caused through negligence of the end-user rather than by sophisticated external attacks. Trust is not a control mechanism, but rather a lazy approach to security. Both Nick Leason (Baring's Bank) and John Rusnak (Allied Irish Bank) were trusted individuals and yet the first managed to destroy a bank whilst the second made the bank's management look foolish. Multiply the potential risk of malpractice by the number of end-users who have access to sensitive data and you begin to appreciate why lazy senior management prefer to repeat the "you have to trust someone mantra" whenever they are embarrassed by a data loss. I would not mind if I could at least see the risk clearly identified on the risk register with the "tolerate" decision box ticked to indicate that they have made a management decision to tolerate the loss. I have never seen this because it would embarrass them to have it so clearly recorded. Much better to come out with the trust paradigm after the loss has occurred. This, of course, is really he fault of the timid risk manager who is too frightened of senior management to tell them of the omission. We auditors have our motto of "trust but verify", which means that we don't trust you until we have verified that the controls really do manage the risk. Sadly, they are often

[1] http://www.rhsmith.umd.edu/faculty/lgordon/Gordon%20Loeb%20Model%20cybersecurity.htm

woefully deficient even for the identified risks, but are totally absent if the risk has not been indentified at all.

John is Managing Director of LHS Business Control, a corporate governance consultancy. He is a member of Council and a former chair of the Information Risk Management and Assurance (IRMA) specialist group. He can be contacted at: john@lhscontrol.com, www.lhscontrol.com, or on +44 (0)1707 851454