Security Divulgence - where's the rub?

In this imperfect world, the buck should still stop with the CEO

By Tony Lock, July 2007

A couple of weeks ago I attended a roundtable, organised to highlight that the RSA Conference Europe event would this autumn settle in London for the first time. Over the course of ninety minutes the panel, unsurprisingly composed of sponsors of the event, discussed many issues. Even though the bulk of the panellists came from a diversity of vendors (RSA, Oracle, Microsoft and SafeBoot) on many issues there was often near universal agreement. But there were also one or two questions on which differences of opinion were visible, especially the matter of "divulgence".

Matters started off with a fair degree of unanimity as panellists discussed the many pressures now acting on holders of data. Whilst all of the usual suspects are obvious and clearly understood, it was interesting to note that without any hesitation everyone present considered that protecting brand values and ensuring brand integrity in the eyes of customers and the public at large have now risen to become one of the primary drivers behind many security initiatives. Even when not declared to be a primary security motivator it is clear that brand protection in the online world is always a matter of concern, and increasingly a cause of security related investments.

Equally interesting was, when I raised the fact that "security solution" technologies on their own cannot secure anything, no one disagreed at all. This was a good job: we have many sources of research insight that clearly illustrate that education in the secure use of all systems, but especially of mobile solutions, is an essential element of any security strategy. There are (too) many instances of people using systems inappropriately and of unsuitable procedures being adopted around systems leading to information leakage. To resolve this, there is a clear need for education to be formalised even around the simple to use systems that are commonly deployed to support core business functions.

Whilst the above topics generated some interesting discussion, they did not result in noticeably different opinions amongst the panellists. But one conversation did prove that there is still room for disagreement. The contentious question is, when to tell customers, partners and perhaps the world at large that something has gone wrong or that systems have been compromised and information has been exposed?

As ever increasing quantities of information is held on IT systems and as both individuals and organisations find themselves "sharing" progressively more valuable data, legislators in many countries are considering under what circumstances data holders should have to let their customers know of security breaches that may compromise the information they hold. In a few countries or states (notably, in the US) it has already become required to inform customers if information held on them may have been exposed; elsewhere, examples such as the theft of a laptop form a Nationwide Building Society employee indicate how some organisations are choosing to disclose security breaches.

One panellist held the view that the CEO and managers of a business should decide, perhaps after consulting with any appropriate regulatory bodies, when or even if, they should notify of information leakage or deliberate data theft. I, along with most of the rest of the panel felt that whilst this might

be the ideal line to adopt it is plainly not going to work unless the CEO has objective, nay absolutely impeccable, judgement and can act in an entirely disinterested fashion. Given the fantastic pressure on CEOs to not only deliver the financial goods but also, as discussed earlier, to protect the integrity of their brand it would be almost impossible to expect them to disclose practically any breach of systems or inappropriate exposure of data that had not already reached the public domain.

To my mind, disclosure legislation will become inevitable in most areas of business. It then behoves us to react reasonably. After all, in nearly all matters of daily life and business we seldom expect everything to always function perfectly. If every organisation can expect things to go wrong, it is up to the organisation to ensure that they have done everything they can to protect their systems, to recognise when they have been breached or data has leaked and to then react swiftly and fittingly to put things right. Part of this means notifying those affected as to the nature of the potential loss, what they should do to minimise exposure and what is happening to prevent future issues arising. While this may not be a perfect solution, we're living in an imperfect world.

About Freeform Dynamics

Freeform Dynamics is a research and analysis firm. We track and report on the business impact of developments in the IT and communications sectors.

As part of this, we use an innovative research methodology to gather feedback directly from those involved in IT strategy, planning, procurement and implementation. Our output is therefore grounded in real-world practicality for use by mainstream business and IT professionals.

For further information or to subscribe to the Freeform Dynamics free research service, please visit www.freeformdynamics.com or contact us via info@freeformdynamics.com.