IT security and Governance

Moving security up the agenda

By Jon Collins, June 2009

Originally published on

The following article was originally published as part of the Freeform Dynamics advisory column on CIO Online. This is focused on the business impact of development in the technology industry. Original articles can be accessed at www.cio.co.uk (registration required).

It has sometimes been said that in Information Technology, the emphasis has been too much on the technology and not enough on the information. This has been particularly apparent in IT security, a part of the IT industry seemingly constructed around telling us about all the things that could go horribly wrong, before rather handily proffering a portfolio of products to resolve the issues.

It could all be so different; we might like to think... but could it? Back in the day, when I had an IT department of my own, I learned just how hard it was to win budget for security related purposes. The question the finance director (and my boss) asked was very simple - "Do we really need it?" And if I didn't have a cast-iron rationale, then the cheque book remained firmly closed. That was then, but the business case for IT security remains as difficult to articulate as it ever was.

Coupled with the fact that there really are bad guys out there - and yes, their attacks really are becoming more targeted - it comes as no surprise that the IT security industry exists as it does. From our research we know that the products that are more likely to be deployed, happen to also be the ones that are simpler to explain - either because the 'threat' really is obvious, or because certain products are generally accepted as being a good thing - anti-virus software is one example, firewalls are another.

All of this does distract from the fundamental point however, that IT security exists to mitigate business risks, not just counter specific external threats. For example, over the years we have repeatedly determined that the biggest threat comes from inside the organisation, either through 'malice or stupidity' of individuals. It does seem strange therefore that so much of security vendors' attention is paid to what happens on the outside, even despite 'technologies' such as data leakage protection being rushed out in response to dropped balls such as the HMRC breach.

While the IT security industry's priorities may be skewed towards what will sell, there are some distinct signs that the industry itself is moving away from the point product model. Arguably, the questions that IT security vendors originally set out to answer, such as what-needs-to-be-secured-and-how, are largely answered today: new technology such as virtualisation and software-as-a-service may bring new threats, but not significant new categories of threat. The result is that such vendors are spending more time working out how to make things work better, rather than what problems need to be solved.

Meanwhile, the ongoing consolidation of security vendors has resulted in integration challenges - both in terms of how security products integrate, and how they work with other systems and applications. Take IBM, for example. Until a year ago the company did not actively market its security technologies as an integrated portfolio, but the picture is very different today. We're seeing

similar stories from EMC with RSA, From Google with Postini, from Microsoft, Symantec and McAfee, and from smaller vendors such as Mimecast.

What we can draw from all of their stories is an acceptance that IT security is not an end in itself. Rather, it offers a means, whereas security of business information is the 'end'. So, what are the outcomes we should be aiming for? It's worth dusting off an old acronym which will be familiar to IT security professionals - Confidentiality, Integrity and Availability. Old it may be, but equally clear is that there is more to C-I-A than can be delivered by IT security alone.

Consider integrity. A couple of weeks ago, I hosted a panel on data integrity at Infosecurity Europe, and what became very quickly clear was that it was almost impossible to separate integrity from a security perspective, from more general concerns about data quality. Similarly, we can look at availability (report). While it may be academically possible to distinguish between service downtime from a denial of service or from a systems failure perspective, the distinction is moot for those poor people who can't get to their data.

Cleary, we need to think beyond IT security if we are to consider - and mitigate - all the risks around business information. But where to start? The answer may well lie in the keyword 'governance' - that word which refuses steadfastly to be defined. Despite its elusiveness, governance appears in discussions around a number of IT topics, not least IT service management and information management, as well as information security. Governance also pops up in numerous conversations around business management, of course.

It is early days for integrating general principles of governance into business in general, and into IT in particular. However, it is clear that IT security stands a better chance of succeeding if it is treated as one element of an IT governance framework, which in turn needs tight alignment with business governance if it is to succeed. This may sound like a glib statement but it really isn't. Having been involved in plenty of conversations through the years about how to raise IT security's position on the agenda, the conclusion reached is that as long as it is seen as an end in itself, it will be doomed to fail.

Don't get me wrong: there will always be a place for technologies to limit security threats, just as there will always be a place for door locks, seat belts and car immobilisers. However, in isolation, such things do not make us better drivers, nor prevent the occasional vindictive attack. It is only by seeing IT security within the overall context of IT and business governance, that it can succeed.

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.