New technology, new risks

An architectural approach to business and IT

Jon Collins, June 2008

First published by
WhatPC?

In a nutshell:

IT strategies are driven by an increasingly holistic understanding of causes and effects. IT Security needs to follow suit

Key points:

- The future of security reflects the future of IT – such trends as offshoring, software as a service and virtualisation will all play their part. Social networking and Web 2.0 are also leading to greater emphasis on the human side of security.
- Just as IT trends are leading to a stronger emphasis on business alignment and systems architecture, so security countermeasures are moving away from point products towards more integrated approaches.
- Risk management has always been a central tenet of good security practice. Organisations looking to adopt a 'joined-up' approach to security, which takes an overview of both business and IT threats, will be best placed to deal with future issues.
- The IT industry, and in particular the IT security industry, would do well to follow suit.

The future of IT security seems like a straightforward discussion – focused, straight and to the point.

Nothing, however, could be further from the truth. Businesses need to understand the risks and implement mitigating strategies if they want to keep ahead of the bad guys.

There are three types of organisation: those who get security and have ongoing risk management activities in place; those that understand security but struggle to implement appropriate measures; and those who think that e-crime will pass them by if they just keep their heads down.

For most, the future of IT security will be much like the present. There will always be people who spend most of their waking hours decoding encryption algorithms and looking for back doors into telephone networks.

But there is also an evolving economy built around the market value of credit card details and the ability to launch denial of service attacks from unsuspecting – and generally poorly configured – home computers.

And IT leaders also need to consider risks caused by their own employees, be they through malice or stupidity. Internal workers have always posed the biggest threat to computer systems – even before product categories, such as data leakage prevention, were posited.

So, what does the future of IT security include? As a starting point, it is worth reflecting on the wider long-term development of technology. There are a number of trends driving how organisations deploy and operate their IT systems – and these threats will have a direct impact on a broad range of areas.

Outsourcing and offshoring

The offshore resourcing market continues to develop, with Indian companies such as Wipro setting up in the UK and other local companies expanding their offshore operations.

Security risks range from the difficulties associated with vetting offshore staff, to the challenge of maintaining business information at offshore locat ions.

Hosting and software as a service (SaaS)

We are not yet seeing wholesale mass adoption of the SaaS model, mainly because the technology is still maturing across areas such as data integration. The risks are similar to the information integrity concerns associated with outsourcing.

Service-oriented architectures and Web 2.0

Both of these topic areas share the risks of using distributed system architectures that may extend beyond the corporate firewall. As well as being open to confidentiality breaches and denial of service attacks, there are also threats surrounding the publishing of interfaces onto corporate systems. In some instances, the interface itself may be confined to company use.

Virtualisation and datacentre automation

Virtualisation offers a quick win for many organisations, helping IT leaders to consolidate applications onto a reduced set of physical servers. The centralised control of preconfigured virtual servers can reduce security risks. But there is also the issue of virtual server proliferation and the potential for mismanagement, which could potentially leave virtual servers open to breach.

Mobility and unified communications (UC)

Suppliers are working hard to deliver on the concept of enabling users to communicate with each other as simply and seamlessly as possible. But UC also presents a two-edged sword, and IT managers need to be prepared for exploitation problems, particularly around spam calls.

Social networking

We are already seeing some of the security challenges that social networking can pose in terms of privacy and identity issues, for example. There are other risks that, to our knowledge, no one has exploited, such as pulling together composite identities of individuals across social networking sites.

Social networking presents a range of personal security issues, but corporate implications across duty of care also create concerns.

The above list of potential risks demonstrates that continued vigilance is only part of the answer. Risk management processes and policies are also crucial, and should be a fundamental part of any organisation's security strategy.

Moreover, all of the above risks share one important element: they affect all parts of the IT architecture. Such risks cannot be mitigated by tactically acquiring a specialist appliance and implementing it in the server room.

If IT security is to be characterised by having a far-reaching impact, so we need to consider how the roles responsible for IT security have a similarly far-reaching remit.

We are already seeing some organisations – HSBC, for example – combining their IT security function with a business fraud function, enabling the institution to deal with business and IT issues from the same point.

I have often characterised IT as a fire extinguisher industry, an analogy that makes sense if all people are doing is fighting fires. Challenges, such as the security issues listed above, will require us to move towards a prevention-based approach rather than a series of poorly-funded coping strategies.

And frankly, given that the trends are happening whether organisations want them to or not, the sooner we can get there the better.

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.