



■ Connectivity, driving productivity requires security rethink, says expert

Technology revolution driving security development

THE changing nature of business, driven by changes in the way people use technology to achieve new levels of productivity, requires a rethink of IT security. That was the broad theme of the opening presentation at IDC's recent business continuity and security in Croke Park.

Eric Damage, research manager, security products, IDC, said that IT was undergoing a major revolution that was characterised by de-perimeterisation, cloud computing, outsourcing and virtualisation. In conjunction with this, Damage said that connectivity is now the main tool for enabling and promoting productivity. He said that Productivity 2.0 calls Data Protection 2.0 that requires a deeper and wider management and control of information flows. In this context, security is not a technical barrier between good and bad, but is rather a business enabler that needs a new business case and return on investment (RoI).

Setting out the current security landscape and market in Ireland, Damage said that software had not yet recovered from the recession. Security hardware markets however, such as unified threat management (UTM) devices and other appliances, were up. Security services, such as

antivirus as a service and the like, had boosted the services market in general. Damage said that according to IDC research, Irish organisations were taking advantage of security as a service ahead of many European countries. He said the adoption path was usually to engage with a service provider by adopting back and recovery services initially. Establishing a relationship, or what Damage describes as an "appetiser", other services are adopted, such as firewall management and compliance auditing. In this manner, organisations get the benefits of reduced capital spend with predictable manageable costs.

Damage said that IDC had conducted research in February and March of this year among 300 Irish organisations. The top three business challenges reported were business survival at 39%, the cost of doing business at 34% and decreases in budget at 19%. Top IT challenges were reported as controlling costs and improving financial situation at 68%, up from 39% from last year, migration from older technology (hardware and software at 14%, down from 25%, and developing and implementing strategies to improve competitiveness at 15%, down from 22% last year.

Damage said that the results

showed a clear understanding of mission in the current climate, namely business survival and IT cost alignment, but the results also indicated evidence of project freeze, with either limited spend or no spend on new projects.

Among the other speakers was Paul Judd, regional director for UK and Ireland, Fortinet. Judd emphasised that modern IT security is "pointless". Referring to what he said was the old culture of "point solution syndrome," he said that network security had to be consolidated to cope with modern threats and trends. Developments such as application specific integrated circuits (ASIC) were allowing "real time, high performance consolidated network protection". He said that for performance in security, scalability was key and that ASICs enabled this.

Consolidated network management and protection was a theme picked up on by Greg Day, principal security analyst, McAfee. He said that there was a desperate need to innovate in IT security to optimise network and security architecture. This optimisation requires multi-layered protection, real time threat intelligence, centralised security management and automated compliance through improved process



Eric Damage, IDC

management. Day said that threat intelligence would mean centralised risk management and modelling to assess threats for one's own organisation.

With cloud computing now a major element of any IT conversation, Damage was urging caution, especially with respect to one major provider. He said that while Web 2.0 was now part of business, highlighting the impact of Twitter and its ilk, particularly in the US market. He said that Web 2.0 "attracts talent". However, he said that organisations needed to be cautious when embracing the cloud and he highlighted the example of Google. He said that despite Google being SANS Institute audited, that it was not necessarily compliant with security standards such as the ISO 27XXX family. Damage advises organisation to ask questions of themselves, their security needs and compliance obligations before embarking on the use of cloud services such as Google Documents.