Network Infrastructure Not Business-Ready

Multiple issues found with configurations, security vulnerabilities and end-of-life status

Sydney, Australia – March 25, 2009 - Poor network management and basic security vulnerability oversights are leaving organisations open to security attacks and operational downtime.This is one of the key findings in the Network Barometer Report launched today by Dimension Data, the $4.5 billion IT solutions and services provider. The Report presents the aggregate data from 152 Secure Network Infrastructure Assessments (SNIAs) conducted by Dimension Data for organisations around the world during 2008, and provides an overview of networks’ configuration, security vulnerabilities and device life-cycle status.According to the Report, 73% of networking devices have known security vulnerabilities which expose a business to both external and internal security attacks and breaches, and which could have significant implications for regulatory compliance. Rich Schofield, Global Business Development Manager, Network Integration at Dimension Data says: “Organisations are running with vulnerabilities they’re probably not aware of. The results also indicate that there’s a lack of process to ensure these vulnerabilities are remediated.”The research also showed that an average of 15 security configuration errors were found per device deployed – despite widely published and recommended standards. “These results are astounding,” says Schofield. “The most basic protection measures against threats which could harm an organisation, such as access and password configurations, are simply not in place. It’s the functional equivalent to leaving the doors and windows unlocked when you leave home,” he explains.And the hits keep coming. The Report also reveals that 43% of all equipment reviewed had entered the first end-of-life cycle stage, and of that group, 56% was beyond either end-of-software maintenance or last-day-of-support. Ageing IT and network assets, depending on their functions, will become increasingly unsupportable and open to risk, leaving the organisation exposed to potential availability and mean-time-to-repair risks. “Today, organisations depend on the functionality, availability and successful management of their IT networks. Indeed, many companies would simply not function without the technologies that enable their business processes,” says Schofield. “Given this dependency, the basics of keeping networks running and ‘ready for business’ should be a priority for most organisations.” For more information on the Dimension Data Network Barometer Report go to www.dimensiondata.com/networkbarometer*PSIRT = APSIRT is a software vulnerability that has been identified by Cisco’s Product Security Incident Response Team-Ends-About Dimension DataDimension Data plc (LSE:DDT), a specialist IT services and solution provider, helps clients plan, build, support and manage their IT infrastructures. Dimension Data applies its expertise in networking, security, operating environments, storage and contact centre technologies and its unique skills in consulting, integration and managed services to create customised client solutions.About the Dimension Data Network Barometer Report The Network Barometer Report presents the aggregate data from 152 Secure Network Infrastructure Assessments (SNIAs) conducted by Dimension Data for organisations around the world during 2008. The Report provides an overview of networks’ configuration, security vulnerabilities, and device life-cycle status. The Report is available for download from www.dimensiondata.com/networkbarometer