Business is ready for networks; are networks ready for business?

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. Given this dependency, the basics of keeping networks running and 'ready for business' should be a priority for most organisations.

Findings from Dimension Data's Network Barometer Report show that managers are placing their organisations at commercial risk by failing to proactively address network asset management.

Basic security vulnerability oversights are leaving organisations open to security attacks and operational downtime		
73% of networking devices are running with known security vulnerabilities	These could expose a business to both external and internal security attacks and breaches, and seriously jeopardise an organisation's ability to meet regulatory compliance	Initiate an ongoing inventory of deployed OS versions and match those to known vulnerability lists. Engage a knowledgeable systems integrator to provide this service on an ongoing basis.
An average of 15 security best practice configuration errors are being made per device	The most basic protection measures against threats which could harm an organisation, such as access and password configurations, are simply not in place.	Although organisations know these are basic requirements, it can be hard to overcome configuration 'drift'. Collect and analyse configurations through using automated systems or engage a partner to assist.
Configuration errors could leave organisations vulnerable to known threats and damage their regulatory compliance objectives		
An average of 30 configuration best practice errors occurred per device	Failing to manage compliance and security at a network level means that organisations are taking a business risk that they're probably not aware of. What's more, these risks are easily remediated.	Ensure there are measures in place for a defined and documented set of: ▲ Network and configuration standards. ▲ Security practices enabled by device features. ▲ Recurring processes to ensure compliance with the documented standards.
Organisations that fail to proactively address network asset management are at commercial risk		
43% of network devices scanned had reached at least end-of-sale status, and **56%** of that group was beyond either end-of-software-maintenance or last-day-of-support.	This means 24% are at significant support and availability risk as equipment beyond end-of-software- maintenance will no longer have newly identified bugs fixed and those beyond last day of support will not be supported at all by the manufacturer.	Adopt a technology lifecycle management planning approach. This will keep the network infrastructure current through a phased approach that doesn't unduly burden any one financial period yet still achieves strategic goals with your network.

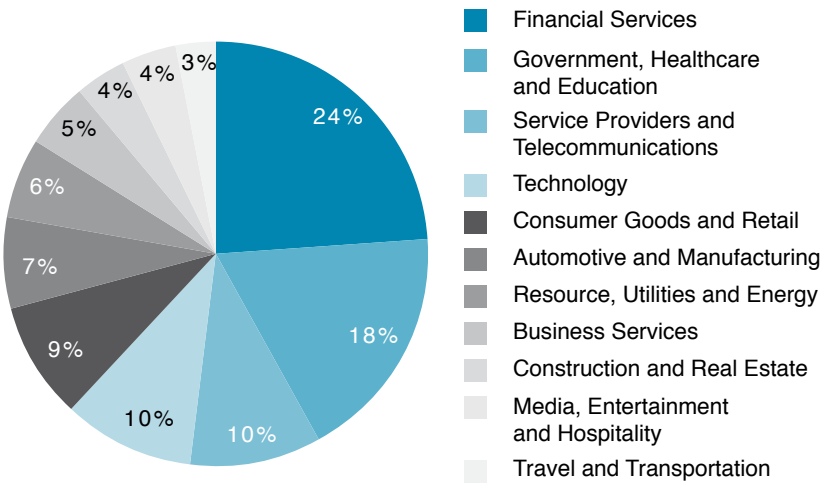
The Network Barometer Report – the first Report published by Dimension Data on the status of networks globally – aggregates data from **152** Secure Network Infrastructure Assessments (SNIAs) conducted by Dimension Data around the world during 2008. The Report reviews networks' readiness to support business by reviewing the security vulnerabilities, end-of-life status and configuration **variance from best practice** of network devices.

Key themes in the Network Barometer Report :

- Vulnerabilities are generally known but not effectively addressed
- Organisations need to align to published best practice standards to minimise risk
- More planning discipline is required in network asset management

Key Sample Statistics:

Sample Distribution by Vertical Industry Sector



Organisations from all regions are represented:

- 36% from Europe
- 22% from the Americas
- 27% from Asia-Pacific
- 15% from Middle East and Africa

Larger and enterprise sized organisations represent the majority of the sample:

- 60% Enterprise sized (over 2,500 users)
- 29% Large sized (more than 500, but less than 2,500 users)
- 10% Medium sized (more than 100, but less than 500 users)
- 1% Small sized (fewer than 100 users)

About Dimension Data's Network Expertise

At Dimension Data we are network specialists. We have designed, deployed and managed thousands of networks for clients of all sizes and from all industry verticals, in almost every country in the world. Based on our experience, the most effective advice we give clients is to have a long-term plan in place to manage their network. Compliance and risk can be managed and mitigated best when you have insight into what's on your network, where it is located and how it is configured, and how much longer it has to operate before reaching end-of-life.

The Secure Network Infrastructure Assessment (SNIA) is a network and security assessment service that discovers, catalogues, analyses network devices. It identifies basic security, configuration and end-of-life issues so that they can be proactively addressed.

For more information about Dimension Data, and to download your free Network Barometer Report,
visit www.dimensiondata.com/networkbarometer