



Intelligent Infrastructure Management a solution for Good Governance

White Paper
Nexans Cabling Solutions
June 2007



Introduction



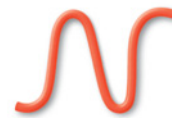
Rob Cardigan
Senior Product Manager
LANsense

With the rigours of Good Governance, Sarbanes Oxley, ITIL and other regulatory compliance, companies have never faced tougher times.

Add to this backdrop the tidal wave of security attacks - both external and internal - and it isn't surprising that of the \$6 billion spent on compliance in 2006, a greater percentage of the budget went to technology, as companies sought to automate and monitor the many controls required.

But for many companies, there's potentially a massive hole in their defences that CEO's are unaware of - one for which there is a simple solution.

The article gives a management-level view of this security weakness and sets out the simple solution that potentially improves the existing return on IT investment, reduces support costs, improves reliability, reduces downtime and provides auditable information for regulatory compliance.



Requirements

There are a number of governance requirements facing a modern business ranging from; Sarbanes Oxley in the financial environment for predominantly US parented companies through the emerging ISO 27001 family of standards for information security management and a raft of other standards, guidelines and industry specific compliance requirements in-between. The one area that all of these initiatives agree is that the provision of control is central to a well managed and secure business.

This is underlined by the recent quote from BCS stating that *"the issue of control is without doubt the single greatest challenge facing business today"*.

The central tenet of all of the "compliance" guidelines and legislation is the ability to provide evidence of control by demonstrating an auditable trail of steps taken to demonstrate conformance.

The IT infrastructure Library (ITIL) methodologies provide guidance on some of the control tools which are available but there is a decidedly slow uptake of ITIL methods in general. Something easily understood and practical is required.

Control of a business' network infrastructure and access to it is an underpinning requirement. One of the key messages from the ISO27001 series of standards is the adoption of a "Plan, Do, Check, Act" cycle (sometimes known as a Shewart or Deming cycle from it's origins in Quality Assurance) as a method of controlling change. Other standards seem set to mandate an improvement in levels of control.

It seems obvious that the physical layer of the network is the key start point for any control activity so it is here that this article begins its examination of one control tool option.

Intelligent Infrastructure Management (IIM) has become something of a buzz term in the IT infrastructure industry but its ability to help solve some of this audit and control requirement is poorly understood.



Tracking changes...

Intelligent Infrastructure Management (IIM) has become something of a buzz term in the IT infrastructure industry but its ability to help solve some of this audit and control requirement is poorly understood.

One of the primary functions of IIM is the provision of change orders allowing an IT team to plan, enact and review for completeness and correctness the physical movement of user devices and associated services around the building. In the course this activity it is the hardware portion of the IIM solution that provides closed loop feedback to “check” the work order. The use of a service provisioning methodology ensures that the right service is supplied to the right device – increasingly important in converged environments where the more complex the network the more sensitive it is to incorrect connection or disconnection.

This issue is of such concern that European infrastructure standards will shortly call for automated connection management and service provisioning in networks of over 1000 floor served points – this is no longer seen as the preserve of the “mega network”!

Added to this work order functionality is the ability to track, in real time, events related to change in the network infrastructure. The use of a discovery engine allows the IIM system to detect the appearance of an IP device and to infer its physical position by correlating the IP and physical infrastructure information. The upshot of this is that the system can automatically place traditional user devices or intelligent building components like access controllers or card swipe points on a floor plan. In a flexible “hot desking” environment the requirement to track the movement of user device becomes an automated task.

All of these events are written to a log, complete with a time and date stamp. This provides an audit trail which details where and when an event took place, with the use of an IP camera or a software link to the CCTV system this can be extended to include information related to who was involved in the generation of an event.

As part of the discovery process the system can also interrogate user device to bring back specific information, for example, a list of installed software or the status of installed operating system updates to help protect against security vulnerabilities.



Cost savings in real time

Because the IIM system updates its database in real time there is also an “always up to date” record of assets attached to the network which makes a physical audit unnecessary under normal circumstances. This is both a time saving feature since a report can be generated in minutes of what is located where and perhaps more importantly auditable evidence of the control of assets.

With the real time logging of events anything unexpected can trigger an alert, perhaps an e mail and SMS or a popup. This means that the arrival of an unexpected MAC address or an unauthorised connection or disconnection in the comms room is automatically flagged to the appropriate person. This can be extended to disable a switch port for an unauthorised device or linked to the security system to provide evidence of the perpetrator.

It is reckoned that some 70% of network downtime is related to the incorrect disconnection of physical infrastructure- someone pulling out the wrong patch cord. IIM provides the planning tools to reduce the likelihood of this happening and the detection tools to enable the rapid corrective action if it does. The old adage that repair is 80% diagnosis and 20% activity no longer applies as only the activity time is significant. Add to the ability to connect to a help desk package and efficiencies in support become achievable.

Integration with environmental monitoring for temperature and power control is possible as is integration with rack management systems to improve physical security in comms room and datacentre environments. Legislation on the power consumption of IT systems cannot be far away and monitoring and reporting of this type of information may well become part of the audit requirement in the future.

There is of course some additional cost but it is estimated that the uplift for an IIM system as opposed to a standard structured cabling system is about 25% which in turn is only about 7-8% of the network infrastructure cost – in total IIM represents a 1-2% increase in the total cost of an IT system. With the efficiencies to be gained from improved change management, reduced diagnosis time and improved service levels a quick return on investment is achievable. Add to this the cost savings realised by not performing physical network audits and this becomes easily understood.



Global expert in cables and cabling systems

Nexans Cabling Solutions

Alsebergsesteenweg 2, b3 - B-1501 Buizingen
Tel: +32 (0)2 363 38 00 - Fax: +32 (0)2 365 09 99

**Nexans Cabling Solutions UK
and Intelligent Enterprise Solutions Competence Centre**

2 Faraday Office Park - Faraday Road - Basingstoke - Hampshire RG24 8QQ
Tel: +44 (0)1256 486640 - Fax: +44 (0)1256 486650

www.nexans.com/lansystems - info.ncs@nexans.com