

Getting physical with network security



Are organisations potentially placing emphasis on the wrong areas of their IT security strategies and are they pre-occupied with detecting network intrusion rather than taking positive steps to prevent it? In this article, Molex's Rob Cardigan* (left) and iTRACS' Rick McNees* (right) suggest that companies are missing a key 'layer' in their IT security strategies – monitoring and documentation of the physical network infrastructure. They put the argument that the need for rapid incident detection, documentation and corrective action is essential, and that modern intelligent infrastructure management systems can provide the solution.



Despite the many IT security technologies now available, security breaches continue to be a major issue for all types of organisations. Security is a business problem, not just an IT problem, and it is not getting any easier. It is a wide and complex area that includes the threat to sensitive information, business systems and hardware.

Large utility companies, as well as the financial services sector, commonly account for the highest rate and severity of attacks. These and many other organisations are spending millions on IT security products. Analysts IDC have predicted the global market for Web intrusion protection products and services alone will reach US\$700 million (£378 million) by 2006. Interestingly however, a recent study by OMB on US Federal Government spending, found little correlation between security spending and actual security.

Why does it matter?

93% of UK firms experienced unplanned downtime in the past year according to a survey of 850 IT managers in the UK. Of those surveyed, 14% suffered more than eight hours of unplanned downtime, with only 17% suffering less than one hour. Minor security breaches – either deliberate or accidental – account for much of this downtime. Many minor breaches, e.g. a lead 'falling out' of a patch panel, may never be traced or the causes ever identified because of poor documentation.

Downtime is very costly. A report by Price Waterhouse Coopers and the DTI on information security breaches revealed that the average cost of a serious security incident was £30,000 and several of those surveyed had single incident costs which were greater than £500,000. This is not a necessary evil; inexpensive solutions for monitoring of the physical layer can reduce unplanned downtime significantly.

The dynamic nature of today's corporate networks means that they are no longer defined by physical boundaries, but instead by enterprise-wide security policies and parameters. To be effective, these policies must include a broad range of security services that govern access to network resources, while protecting these same resources from internal and external threats.

Almost all network security devices installed are aimed at defeating external threats, but perhaps the most common and most serious security breaches are caused by internal parties. In this case, intrusion detection systems are voided, as the culprits already have systems' authorisation granted to them as employees. Of 530 security practitioners polled by the FBI in the 2003 *Computer Crime and Security Survey*, 80% reported unauthorised access to systems by insiders.

Controlling activity and access of people already inside is a big problem. Insiders know the company's assets, where they are and their value. Costly thefts of confidential information such as personnel records, financial details, and research & development information are easily achieved by people on the inside with knowledge of the environment and the technical means to navigate the network – much more so than external hackers.

The many security challenges that exist today fall broadly into the following categories:

- **Unauthorised devices** – Devices attempting to connect to the network that are not recognised or authorised – these may include unauthorised devices or users, or authorised users innocently connecting a wireless access point into the network which could introduce potential security vulnerability from devices accessing the network through that connection point.
- **Non-compliant devices such as mis-configured systems** – systems not updated with latest vendor releases security fixes or proper anti-virus files.
- **Unauthorised activities from internal users** – accidental or deliberate actions by employees or ex-employees that compromise services or information.
- **External users** – viruses, worms, denial of service and hacker penetration.

- **Physical theft** – physical theft of hardware/software.
- **Fraud** – bogus payments and false credit details.
- **Proprietary information** – destruction or copying of company data.

Deploying a layered security solution helps protect organisations from this plethora of security challenges. There are three 'layers' to enterprise IT:

- **People** – including employees, customers, partners and the general public.
- **Applications** – including email, procurement, ERP and supply chain.
- **Network infrastructure** – including routers/switches, mainframes, virtual private networks.

A good security strategy needs to consider all levels. Companies continue to spend vast amounts of money on protecting the people and application layers but often overlook the network infrastructure level.

Intelligent infrastructure management

Maintaining physical infrastructure security is now a very simple process with the sophistication over the last year or so, of intelligent patching technology. Intelligent patching provides a vital layer of protection enabling rapid detection, documentation, notification and corrective action. Such a system can be used to document and monitor the network in real time, warning of any

unauthorised connections/disconnections, entry to computer areas etc. Layer-one documentation and monitoring can protect against certain unauthorised activities by correlating devices and their physical location in the organisation. Some activities or devices may not be authorised in certain locations.

Traditionally, a network manager had the time consuming and almost impossible task of keeping an accurate paper record of all physical network connections and any moves, adds and changes (MACs). This may be in an office of 50 people or 5000 people – in a single office or hundreds of small offices spread throughout the world. Companies with high staff churn rates put further pressure on the number of MACs required. The data is in many cases drastically out-of-date as manual upkeep is often overlooked in the bustle of everyday business. What's more, it is not uncommon for a company to outsource its entire MAC operation. One such company has been known to accept and tolerate that 15% of its contract information is wrong and pays additional service call charges for the contract or to change and document the fix. As well as the obvious security issues with inaccurate documentation, it is also far more expensive.

With intelligent infrastructure management technology all devices connected to the network are automatically detected and electronically logged, as are any changes in network connections, including security wiring. Network connections can be correlated with physical location of network access point. This means that the deliberate or inadvertent disconnection of a key patchcord can be fixed in minutes, saving thousands of pounds by minimising downtime.

In addition, security devices such as cameras, access switches and motion detectors can be set-up and correlated with network event and access logs. For example, any unauthorised persons entering the comms room are recorded in real time by a camera and alarms or alerts can be triggered for immediate response against unauthorised activities.

Using accompanying software, modern intelligent infrastructure management systems identify faults and any potential espionage in real time. These systems can detect when a device is connected to the network providing vital information, such as the host and IP address, to the network manager. This can be matched with exact location of the device down to the jack/wallplate to which it is connected. Network connectivity can further be checked against business rules – authorisation, event schedules and work orders.

In remote sites, particularly where the network manager isn't always present, the ability to monitor and track infrastructure





The addition of intelligence infrastructure management to the cabling system turns it from a flexible network to a powerful controlled infrastructure.

and equipment centrally with instant notification of remote connectivity changes and their root cause, is a key security advantage. The costs of remote site monitoring are dramatically reduced through the ability to diagnose or direct connectivity changes without dispatching a technician. If maintenance is required, the dispatched technicians can arrive prepared and equipped to execute MACs. Those in charge of security can have the peace of mind that, at remote sites, access is secured and that all access and connectivity is tracked and logged.

Intelligent infrastructure management also helps organisations maintain business continuity in the event of an uncontrollable security breach. In a disaster recovery situation, modern intelligent

infrastructure management systems provide a 'snapshot' of the full connectivity requirement of the affected organisation. This feature is proving to be an invaluable aid for US Government agencies that are establishing alternate computing facilities for ensuring operations continuity. For example, when the US Senate faced the Anthrax scare that closed several offices, it was able to accurately replicate connectivity and networks services at its alternate facility to help maintain levels of continuity and security.

Conclusion

The addition of intelligence infrastructure management to the cabling system turns it from a flexible network to a powerful controlled infrastructure. An intelligent

solution with real-time feedback can make a significant contribution to the security, business continuity and downtime of an organisation.

With ever-growing security threats, a preventative, layered approach to security by organisations is key. Modern intelligent patching systems enable physical network infrastructures to be built and trained to detect intrusion from the potential threat of internal espionage before it occurs rather than after.

Consideration of the following questions will help the IT manager when planning infrastructure security:

1. Can I detect unauthorised devices in real time including their physical location?
2. Can I automatically detect the root cause of an unscheduled disconnection of a critical device?
3. Can I enforce the compliance with prescribed security policy of a device connecting to the network?
4. Do I have the capability to deny an unauthorised or non-compliant device access to the network to prevent a potential threat risk?
5. Does my security plan take the physical infrastructure into account?
6. Is my network layout designed to be secure from intrusion?
7. Have all the policy and procedures for physical and connectivity access been documented for employees, contractors and service technicians?
8. Do my consultants and installation contractors have documented security policies and procedures in-line with mine?

9. Do our mission critical devices require higher security media such as fibre?
 10. How would I be aware of a security breach in my physical network and shut it down?
 11. Does my disaster recovery plan incorporate structured cabling requirements?
 12. Does my network infrastructure use products with security features (i.e. colour-coded patch cords and modules, locking covers, termination mounts and/or pre-terminated fibre products)?
 13. Do I have a real time schematic of the structured cabling installation including active ports?
 14. Are all of my organisation's floor-plans, hub-room drawings and port assignment documents up to date and in a secure location?
- Currently, intelligent infrastructure management systems are able to tell the physical location of a device. With new enhanced software soon to be available, the system will be able to correlate activity or behaviour of the device with its physical location and flag any unusual or unauthorised activity, e.g. why is this person logging on from this other person's machine or office location?

About the authors:

Rob Cardigan is technical manager at Molex Premise Networks and Rick McNeis is global marketing manager at iTRACS.



Faced with a problem?
Fed up with being passed
from supplier to supplier?

Case Communications

Solutions for systems – not just boxes
Experience

Supporting systems since the 1970s.
Support for Cisco, 3-Com, eXtreme, Nortel, Lucent
Avaya, Nortel, Cray/Case, PCs, Servers, SW Roll Outs.

UK Wide Coverage
Responsive

4 hour response available in most locations

Reduce Operational Costs by up to 20%

Introductory Offer
Network support review
Value Over £1,000
Free for first 5 enquiries

Case
Communications

Tel +44 (0) 1494 833 740
Mail support@casecomms.com
Web www.casecomms.com

Network monitoring, admin and protection package

Navigating the compliance and regulatory minefield is becoming increasingly difficult as new Acts and Guidelines – such as Gramm-Leach Bliley, HIPAA, Sarbanes-Oxley, and Basel II – place further demands on organisations to restrict access to confidential information and/or enforce security policies.

Designed to allow network administrators to properly safeguard and monitor their networks by incorporating network documentation, asset management, network monitoring, and vulnerability management features, is the latest version of Neon Software's *LANsurveyor v 9.0* for Windows.

This product enables users to first identify and then safeguard and monitor what is on their network. A number of new features have been added, including the *Continuous Scan Intrusion Detection System* (available as an add-on module), which integrates with vulnerability assessment tools from Microsoft, Symantec and Qualys.

Map Levels enables users to switch between three different map views by clicking the appropriate icon, while a *Show/Hide Nodes* feature means that nodes connected to routers or switches can be shown or hidden selectively.

Rogue nodes that may not be identifiable using ICMP or other discovery methods can be detected using *Continuous Scan*, which also now logs information about nodes that connect to, and disconnect from, the network in the session log. This information can be used to document network usage, threats, and

system availability.

Continuous Scan also gives the option of authenticating newly found network nodes. It discovers vulnerabilities and ensures compliance of those new nodes using Qualys' *QualysGuard* and Microsoft's *Baseline Security Analyze (MBSA)*. If the new node fails authentication, *Continuous Scan* identifies the node as 'un-authenticated' and takes the actions specified.

TCP port monitoring will alert administrators when critical network services go down, and more alert options (e.g. launch an application or a file) with alert limits mean that different personnel can be called during the workday, weeknights and weekends.

In addition, *LANsurveyor 9.0* includes SMTP authentication, enabling to be sent via SMTP servers.

With *LANsurveyor 9.0* a variety of information can be integrated very quickly and easily.

"Not only does it provide SNMP reporting, but also there are reports that provide Layer 2 and Layer 3 integration information (Switch/Hub Ports report) as well as hardware and software asset reports (installed software, CPU, RAM, disk information, etc.)," comments Craig Isaacs, president at Neon Software Inc.

"New in *LANsurveyor 9.0* is support for APC's most important UPS MIBs. Create a custom report with a few clicks that shows battery health, run time, current power status, percent load, and more."

Prices start at £275 (exc. VAT).

More details: 01798 873 001