■ Infrastructure Management & Monitoring for *Business-Critical Continuity*™

Branch Infrastructure Management

Challenges and solutions for centralized remote office management

Avocent®

EMERSON™
Network Power

Branch Infrastructure Management

Table of Contents

Executive Summary

Remote offices face a number of unique challenges. Specialized hardware and software operate at each remote office site, often requiring IT knowledge to manage. At some sites, a non-standard IT infrastructure–installed because of decentralized purchasing or other legacy issues–poses additional complexities. Most importantly, many remote office sites cannot justify the degree of IT support necessary to ensure smooth operation and proper crisis management. As a result, typical remote office IT management is cumbersome, expensive and insecure, with inadequate procedures and hardware in place.

The true cost of downtime varies greatly from business to business and outage to outage. Still, following simple guidelines, IT managers can ascribe values to lost productivity, labor costs, short-term and long-term business losses and remediation costs to scope out a high-level understanding of the true cost of failure at remote offices.

Traditional methods of addressing remote office IT equipment or software failures include hardware redundancy, in-band monitoring and simply accepting a greater degree of risk and failure as the cost of doing business. Each approach presents its relative virtues, but individually or combined, all fall short of a comprehensive, cost-effective solution, leaving a business open to financial loss.

Simple Remote Management Infrastructure (SRMI) is a comprehensive suite of out-of-band remote office management tools. Centralized IT staff can be virtually "in front of the terminal" at each remote office. SRMI provides the monitoring, diagnosis, configuration, security and power management necessary to enable true central management of remote locations.

The Challenge of Remote Office Management

Remote offices are unique. Their specialized infrastructures often require a large amount of IT attention, but they frequently operate without any IT staff at all. As a result, remote office management is often cumbersome, expensive and insecure, with inadequate procedures and hardware in place to manage crises, ensure policy and enable regulatory compliance.

The size of a remote office, the degree to which its work is business-critical and the availability of qualified local employees all factor in to IT staffing decisions. Smaller offices, or those with very little high-profile work, may not be able to justify a dedicated staff. Certain hardware and software specific to the remote office environment, such as POS terminals or credit card readers, may require special skills unavailable in a local IT pool. For these and other reasons, most remote offices cope with limited resources or share a regional staff with nearby offices.

In the absence of a dedicated IT staff, users may begin to self-administer workstations or perform other basic IT functions such as power cycling at times when an on-site visit is impractical. Day-to-day operations of this sort can lead to policy and process breakdowns and render the central IT department unable to audit the history of device configurations and access.

Some remote offices add to their IT resources independently, without guidance from the central office, while other remote offices enter the company through acquisitions or partnerships. These issues can produce non-standard hardware and software environments. This limits visibility from the central office and further complicates remote management. Many remote office applications and devices provide no remote administration tools, and others provide information only when the monitored system is functioning properly. As a result, even simple outages that might require only a system reboot can require an on-site visit to diagnose the problem.

Downtime at remote offices is expensive and risky. According to Nemertes Research, the average on-site visit, or “truckroll,” by an IT administrator costs between $500 and $2500, but the true cost of an outage can be far greater. While large central offices can often failover services and applications to other hardware and networks, many remote offices rely on a single set of hardware and software. An outage at a remote office can shut down productivity completely.

Remote outages can also create security holes with far-reaching consequences. Without visibility into the remote office, administrators have no audit trail for device, file and network access, and inoperable security devices such as firewalls can leave sensitive data at risk from outside attackers.

Each industry has unique costs associated with remote office failure. For commodity service businesses such as retail and financial services, downtime may lead to customer abandonment. These and other highly-regulated industries may be subject to fines and other penalties for violating the security and privacy standards of their relevant commissions. Service providers may also violate Service Level Agreements with customers, leading to financial penalties.

Existing Remote Office Solutions

Traditionally, IT administrators have dealt with remote office administration through hardware redundancy, in-band monitoring or modifying their expectations of acceptable risk. Each approach has its relative virtues, but individually or combined, all fall short of a comprehensive, cost-effective solution.

Hardware redundancy

One of the simplest ways to protect against hardware failure is to locate backups for critical hardware on-site. For certain classes of hardware, most notably hard drives, this strategy works well. Hard drives are inexpensive commodity items, generally providing ample warning before failure, with mature standards such as RAID to automate backup drive maintenance and failover.

For other, more complex and expensive classes of hardware, hardware redundancy is impractical. In the absence of RAID controllers or their equivalent, maintaining mirrored hardware configurations requires administrators to configure multiple devices with identical settings, patches and add-ons. This overhead is difficult to justify in a remote office that is already short on IT staff.

Even a complete, on-site backup requires an IT staff member to exchange parts, and duplicate hardware cannot help the central office diagnose problems stemming from application configuration or connectivity. Most large enterprises upgrade their support contracts to provide fast replacement of expensive, critical hardware, but even these contracts require on-site IT staff to diagnose the problem before the vendor will dispatch a replacement.

In-band monitoring
IT administrators typically monitor remote office infrastructure using IP-based or dial-in management software. This software takes different forms, including virtual terminal servers, telnet sessions or browser-based consoles. Some server vendors offer embedded management hardware cards in their systems that provide detailed environment information and device-level configuration options to a custom application.

While these tools are extremely useful for troubleshooting and routine configuration, any functions requiring a physical presence at the machine itself, such as a power cycle or a CTRL-ALT-DELETE reboot, are generally unavailable. Learning and managing a separate application for each piece of hardware is a difficult, time-consuming process. Most importantly, most existing remote monitoring tools are “in-band” technologies, relying on the proper operation of the hardware and network they monitor. If a piece of hardware or a network connection fails, remote management tools are unable to communicate.

Acceptable risk
With no comprehensive, affordable solutions available, a surprising number of businesses choose to endure lower levels of performance at remote offices. By lowering expectations of remote office productivity and accepting downtime for even the simplest power cycle, businesses change their threshold of acceptable risk and tolerate a greater degree of failure.

Businesses without a remote management strategy leave their operations vulnerable, with no early warning of problems at the remote office and no remote diagnosis or remediation tools. Outage occurrence creates a heavy dependence on expensive outsourced IT staff or under-prepared in-house labor.

Scoping the Problem

Most IT managers have not calculated the cost of downtime at their remote offices. While every business, office and outage is different, the following guidelines allow businesses to understand the high-level costs of remote office failures and create appropriate budgets for preventive measures.

- Lost productivity: In its simplest form, lost productivity is the product of the number of a worker’s productive hours lost to an outage and the worker’s salary per hour. More sophisticated calculations measure the financial impact of lost productivity (e.g., lost profit from the work that would have been produced during the outage) or subtract the relative value of alternate work performed during the outage from the base calculation.
- Additional labor cost: These include outsourced IT, overtime for all affected staff, transportation of IT workers to the remote site or remote workers to an alternate location and the cost to other projects of IT staff reassignment during the outage.
- Short-term business loss: Any sales or service revenue lost at the remote office during downtime.
- Long-term business loss: An estimate of customer abandonment costs that might occur as a result of downtime. These are very industry-specific and business-specific, so IT managers should look to previous outages within their business or sector for estimates, if possible. Long-term business losses are particularly important to commodity businesses without physical goods, such as financial services.
- Remediation costs: This includes any fines, judgments and legal fees incurred as a result of an outage, as well as any crisis management costs and advertising aimed at restoring consumer or partner confidence.

SRMI: A Comprehensive Solution

SRMI is a comprehensive suite of out-of-band management tools for remote offices. It provides the monitoring, diagnosis, configuration and power management necessary to enable true central management of remote locations.

Key features of SRMI include the following:

KVM over IP
Keyboard, video and mouse (KVM) technologies allow administrators to interact with multiple devices through a single console, saving rack space, power, cabling and time. KVM over IP provides the same BIOS-level functionality to remote administrators via the Internet, a VPN or any other IP network. This allows administrators to view error messages and the screens of hung devices from the central office, reboot the device and perform any necessary maintenance–even at the BIOS level–as if they were in front of the device itself.

Remote, out-of-band power management
KVM solutions alone are unable to reboot devices that do not

respond to keyboard or mouse input. True SRMI requires a remote power management interface to cycle power on hung devices or restart devices after power outages.

Virtual media
Virtual media is a remote-manageable storage solution that functions as a virtual hard drive or optical disk. It allows administrators to install software and updates to multiple on-site devices without the overhead, shipping concerns or security risks of physical media.

Serial device support
POS devices, credit card scanners, time clocks and other hardware are just as important to a remote office's function as servers and desktop computers. Businesses often use specific hardware, and a true remote management system must be able to manage it all.

Cross-vendor unified console
Vendor-based management solutions are unique and incompatible with other management systems. A true SRMI system must be able to monitor and control devices from a wide range of vendors and provide a single, unified console to display a comprehensive view of an office's status.

Security and access logging
Through its unified console, SRMI should provide an audit log for every connected device. It should also allow administrators to enforce security policy across all connected devices from a single screen, while working with existing authentication and encryption configurations.

By placing central IT staff "in front of the terminal" at each remote office, SRMI allows businesses to do the following:

- Realize the full potential of high-value IT workers with specific knowledge by giving them simultaneous access to all remote locations
- Reduce the number of untrained or undertrained staff configuring and "managing" remote office IT assets
- Eliminate the need for on-site visits for power cycling and other simple out-of-band fixes
- Assess the severity and collect the details of a problem before alerting outsourced or roaming IT staff
- Ensure policy and regulatory compliance across all offices without time-consuming audits
- Provide a centralized, standardized audit trail of device uptime, access and upgrades
- Lock out unauthorized users

References

"Convergence and Next-Generation WANs, Vol. 5: Branch Office Best Practices," Nemertes Research, Inc.

About Emerson Network Power

Emerson Network Power, a business of Emerson (NYSE:EMR), is the global leader in enabling Business-Critical Continuity™ from grid to chip for telecommunication networks, data centers, health care and industrial facilities. Emerson Network Power provides innovative solutions and expertise in areas including AC and DC power and precision cooling systems, embedded computing and power, integrated racks and enclosures, power switching and controls, monitoring and connectivity. All solutions are supported globally by local Emerson Network Power service technicians. Aperture and Avocent solutions from Emerson Network Power simplify data center infrastructure management by maximizing computing capacity and lowering costs while enabling the data center to operate at peak performance. For more information, visit www.Aperture.com, www.Avocent.com or www.EmersonNetworkPower.com.

Emerson Network Power.
The global leader in enabling *Business-Critical Continuity*™.

EmersonNetworkPower.com

- AC Power
- Connectivity
- DC Power
- Embedded Computing
- Embedded Power
- Infrastructure Management & Monitoring
- Outside Plant
- Power Switching & Controls
- Precision Cooling
- Racks & Integrated Cabinets
- Services
- Surge Protection

0810-BIM-WP-EN