

## Tech & Trends

---

### General Information

April 20, 2007 • Vol.29 Issue 16

Page(s) 25 in print issue

## Remote Data At Risk

### How To Defend Data In Remote Office Environments

Enterprises funnel loads of time, money, and energy into the process of protecting in-house data, and for good reason—the existing threats to data are numerous. Yet the moment an enterprise situates employees outside those walls, the rules of protection change because processes for securing in-house data don't always apply to remote office locations.

“About 60% of all corporate data is in remote offices and out of the IT department's control,” says Tom Mackowski, vice president of digital product management for Iron Mountain ([www.Processor.com/IronMtn](http://www.Processor.com/IronMtn)). “Remote office data, also known as ‘distributed data,’ lives at the edge of the network on remote servers and PCs—typically outside the layers of traditional security afforded to a data center.”

In many cases, that remote office data is no less important than in-house data because enterprises must distribute reports, statistics, and other information to remote workers in order to facilitate an effective communication pipeline. Further, these employees typically have unfettered access to in-house data, which means that any breach of that connection could spell doom for enterprise security.

#### ■ Challenges Ahead

According to Scott Ksander, chief information security officer and executive director of network services for Purdue University, there are three basic problems with remote office technical configurations. The first issue deals with the path leading from the main office to the remote office.

“Economic requirements often drive this to some sort of ‘commodity Internet access’ rather than a dedicated path,” Ksander says. “If those economic requirements exist, a fully encrypted virtual private network is still a must. Without this, data is at risk as it moves.”

The second problem, Ksander says, is determining a method for providing effective IT support for the remote office. Enterprises might discover that support requirements in the main office can be difficult to maintain in the remote office, and if those requirements aren't fully implemented or understood, data will be at risk as it rests.

“The final element of protection is physical protection. Server rooms, office environments, and wiring closets may be less secure in a remote location using leased space designed for general office environments and not IT machine space or secure IT storage,” he says.

Dave Elliot, vice president of worldwide marketing for Arkeia Software

([www.Processor.com/ArkeiaSoftware](http://www.Processor.com/ArkeiaSoftware)), explains that remote offices tend to create what he calls the “elephant through the garden hose dilemma,” in which huge data growth at the edge of the enterprise—along with the emerging requirements to protect that data—presents challenges for companies looking to move large amounts of data across a limited network.

## ■ Protection Plan

Naturally, there are basic, no-brainer options, such as fully encrypted VPNs, available to enterprises looking to secure remote office data, but other methods can also contribute to an end-to-end protected remote environment.

“Centrally administered software support [from the main office], while expensive on the surface, can save money in the long run on support and reduce the risk of weak or misconfigured remote computing equipment,” Ksander says. “There are many products from various vendors, as well as products native to operating systems (such as Microsoft’s SMS), that provide central administration.”

Because any locally installed software can introduce risk, Ksander recommends that enterprises keep operating system and applications software patched to current levels. Further, they should utilize antivirus and antispyware products and software- or hardware-based firewalls (or both).

To avoid the risk of PC and laptop data falling into the wrong hands, Mackowski says that enterprises should consider encrypting sensitive data, but they can also choose the less burdensome method of implementing more active technologies that monitor for abnormal or threatening behavior and destroy sensitive data before unauthorized parties can access it. He also stresses the need for centrally managed online backup, which takes the responsibility away from the employees and gives it back to the IT administrators, and using online backup to secure data on distributed servers.

“There are a number of products and services available on the market for protecting data, but the key factor is ease of use without sacrificing the important enterprise features that are required,” says Josh Coates, founder and CEO of Berkeley Data Systems ([www.berkeleydata.com](http://www.berkeleydata.com)). “Remote backup is by far the safest and cleanest method for dealing with remote offices, especially if the service has a simple, centralized method for configuration and monitoring.”

When selecting an online backup service, Coates suggests that IT managers carefully consider encryption features. For example, remote backup becomes far safer when companies use private encryption keys unknown to the backup vendors. “Private encryption prevents anyone—from a disgruntled employee to [Vice President] Dick Cheney—from snooping around in confidential corporate data,” Coates says.

## ■ System Surety

Companies should also work to ensure the systems holding their remote data are in good condition and can withstand potential disaster. According to David Weiss, CEO of Dataprobe ([www.dataprobe.com](http://www.dataprobe.com)), fault tolerance and redundancies can be built into most systems and processes, and standard techniques such as RAID arrays, high-availability clustering, hot sites, and protection switching can be deployed to provide alternate resources.

“The protection and uptime of remote systems is not just important for an organization; it is absolutely critical for business continuity and long-term success,” Weiss says. “In today’s fiercely competitive market and fast-moving economy, it can mean the difference between success and failure for a company.”

Remote data protection is no small feat, and Arkeia Software’s Elliott warns these

endeavors can entail plenty of costs beyond just time and effort: “IT managers must take into account the entire cost of new architectures, including the learning curve and the ongoing management of the solutions.”

Nonetheless, by considering all angles and deploying the necessary technologies, enterprises can certainly enjoy the benefits of remote office production without worrying about the potential demise of their data. ■

*by Christian Perry*

## Getting Employees On Board

Getting the technologies in place to protect remote office data is one thing, but getting employees onboard with the new security efforts is an altogether different beast. However, this process is far from impossible, and Iron Mountain’s ([www.Processor.com/IronMtn](http://www.Processor.com/IronMtn)) Tom Mackowski says that automation and training are key to success.

“If there are opportunities to automate a process, it’s in your best interest to do so,” Mackowski says. “However, you’re not going to be able to do that for all processes—that’s part of the challenge. For processes that are not centrally managed or automated, hold management training sessions so everyone understands their specific role and its importance to the company.”

Purdue University’s Scott Ksander agrees and adds that policy is similarly integral. “Provide professional development for remote office IT staff if central IT maintenance is not available or funded,” he says. “Have clear, effective policies that specify remote policies, procedure, and best practices.”

## Protection Checklists

Enterprises should construct a detailed plan for protecting data in remote offices, and Purdue University’s Scott Ksander and Berkeley Data Systems’ Josh Coates provide technology checklists to help them begin the process.

### **Ksander**

- VPN
- Firewall (hardware, software, or both)
- Fully current operating systems with periodic patching
- Fully current application software with periodic patching
- Antivirus software with regular virus definition updates
- Antispyware software with regular spyware definition updates

## Coates

- Secure, remote backup service
- Private-key encryption
- Open-file support
- Centralized configuration management
- File versioning
- Block-level differential backups

## SPONSORED LINKS

### Adaptec Snap Enterprise **Data Replicator Advanced**

Powerful remote data management: high-performance, network-optimized software solution for managing and reporting on business-critical information throughout a distributed enterprise

[www.Processor.com/SnapEDR](http://www.Processor.com/SnapEDR)