



I D C T E C H N O L O G Y S P O T L I G H T

Endpoint Data Backup and Security: The Growing Need for a Better Approach

March 2011

Adapted from *Protection and Recovery of PC Data: The Intersection of Desktop Virtualization, Security, and Storage* by Laura DuBois, IDC #221174

Sponsored by Copiun Inc.

With the rapid expansion of mobile devices on corporate network endpoints, companies are increasingly challenged to provide an enterprise data backup and recovery strategy that will deliver greater efficiencies to data management, improve data backup costs, and maintain a secure environment. This Technology Spotlight discusses the key issues surrounding the changing user environment and the resulting need for improved data backup and security. Additionally, it examines the critical concerns companies face as they support occasionally connected users across a distributed network. The paper looks at the technologies offered by Copiun Inc. in this strategically important market.

Introduction: Growing Mobile Work Environment Exposes Backup Weakness

As knowledge workers turn to a variety of mobile devices to get their jobs done, IT organizations are not keeping pace when it comes to incorporating these devices into a comprehensive corporate data backup and recovery strategy.

No company can afford to delay a backup strategy that responds to this new landscape of mobile devices. As IDC research shows, portable devices accounted for 55% of PC unit shipments in 2009, a 15% year-to-year increase. During that same period, shipments of desktop units slowed by 17.3%. The implication is clear: Backup strategies not only must efficiently manage data residing on a complex mix of endpoints across a corporate network but also must accommodate devices that are only occasionally connected to the network.

The current approaches to PC backup and recovery show weaknesses that could expose companies to a host of problems. More than half of IT and business professionals surveyed by IDC reported that their companies use software or a service provider for PC backup. However, nearly one-third of the survey group continues to rely on users to back up their own data. Significantly, nearly 14% are not backing up PCs at all.

To date, many companies have deployed backup tools because of concerns about hardware failures and data loss. Some companies also report using PC backup tools because of their need to address legal or regulatory mandates.

Additionally, companies are clearly beginning to grasp the importance of a sound PC backup and recovery strategy. Nearly half of the respondents in the survey classified PC data loss as "serious" or "extremely serious."

IDC research shows that these concerns are valid and are only magnified by the increasing use of mobile devices. Without a comprehensive backup strategy, companies face not only monetary losses from lost equipment or data but also other threats with far-reaching consequences, including the following:

- Noncompliance with regulatory and legal mandates
- Decreased worker productivity
- Damage to a company's brand and reputation
- Loss of customer and shareholder confidence

Centralized and Comprehensive Data Backup and Security

While many companies currently use some backup and recovery software, their strategies are often incomplete. For example, today's strategies often do not take into account the needs of the occasionally connected user. This leaves an organization vulnerable to problems such as viruses and system failures.

Also, IDC research shows that among companies using a software tool for PC backup and recovery, 20% still require some kind of user involvement in their backup procedures. This means that users must move or copy files before a backup is initiated. The potential for human error and resulting backup or recovery problems is a significant factor for these companies.

However, IDC has determined that companies are beginning to invest in technologies that will enable them to more centrally manage PC backup and recovery. This shift indicates that IT is beginning to recognize how mobile devices are changing the requirements for endpoint backup and recovery. In many cases, a more centralized approach offers advantages, such as risk mitigation and allowing IT to control remote assets. This is all the more critical because tablets and other small handheld devices can create an even greater risk of theft or loss.

Intersecting Trends Demand Better Backup and Recovery Strategy

The emerging backup challenges are the result of several trends and factors that together render the traditional approach of scheduled backups ineffective.

Companies are becoming more accepting of mobile devices, such as smartphones or tablets. IDC research shows that the mobile device management market will grow steadily in the next five years because of this acceptance. Further, the worldwide market for remote access services software is expected to grow from \$155.4 million in 2009 to \$227.6 million in 2014 at a compound annual growth rate of 7.9%.

Meanwhile, mobile devices are increasingly becoming the tool of choice for users to work with critical and proprietary data while they do their jobs remotely. IDC research shows that IT departments are increasingly permitting individuals to use their personal devices to get access to corporate applications and data. Evidence suggests that companies that have been resistant to personal devices are now becoming more open to the inevitable usage of mobile devices.

In many cases, however, a corresponding IT-driven backup and recovery plan is not yet in place.

Compounding this challenge for IT organizations is the need to provide backup and recovery services in a timely fashion. Users' expectations for few disruptions in service only continue to grow. IT needs to assess how to best provide acceptable RTO in large, distributed environments. The challenge will be to implement a centralized backup strategy while delivering backup and recovery services within tolerable time frames.

Considering Copiun Data Manager

Copiun Inc., based in Marlborough, Massachusetts, was founded by former EMC managers. It was recognized by the MIT Sloan CIO Symposium Innovation Showcase as one of 10 early-stage companies with innovative technologies for IT. In addition, the company's flagship product, the Copiun Data Manager (CDM), was nominated as a 2010 Backup Product of the Year by SearchStorage.com/*Storage* magazine.

CDM is an enterprise data management solution designed to enable IT to regain control over a rapidly changing end-user environment populated with a complex array of mobile devices. According to the company, CDM can provide up to 95% storage and bandwidth reduction with its global, object-based deduplication technology.

The software addresses the following key areas:

- Backup and recovery
- Risk assessment
- Federated search for ediscovery of endpoint data
- Universal data access from tablets/smartphones

Copiun's key differentiator is its object-based deduplication technology, which eliminates duplicate data globally and at the source, providing both storage and bandwidth savings. The company positions its software as superior to existing block- or file-level deduplication solutions because it's able to detect embedded common objects across unrelated files anywhere on a company's network. For example, a company's logo may appear in a variety of documents, such as letters, memos, or presentations, created by different departments. The logo is stored and transmitted as unique data only once. Copiun accomplishes this by "chunking" files by native objects such as images, attachments, slides, or paragraphs. In contrast, other approaches define logical or physical layouts of data.

Other key product features include the following:

- **Initial backup solution.** Copiun offers a "seeding server" option, a portable device that can be shipped to a remote site, where the first backup is done over a LAN to the seeding server. All the data on the seeding server is encrypted and shipped back to the main site. It is then uploaded to the main server.
- **LAN-speed recovery for distributed sites and support for mobile users.** The software provides nearly continuous backup for mobile users whether they are directly connected to the corporate network or linked to it via a VPN or a public WiFi connection. In addition, the company offers a Cache Server option that allows data recoveries to take place at remote sites over a LAN, greatly improving RTO for bulk recoveries at remote sites.
- **Infrequently connected user support.** To accommodate users who are connected to the corporate network only occasionally, the company offers the Constant Access Gateway (CAG). This technology allows companies to securely back up mobile data even when users are not connected to the corporate network via a VPN. In this case, data is backed up to the CDM Server behind the firewall and inaccessible from the outside. As a result, no incoming firewall ports need to be opened.

The CDM Server establishes an outbound connection to the CAG Server using specific connection parameters. A secure control channel between the two is then established. When a mobile user connected to the Internet then connects to the CAG Server, it in turn communicates to the CDM Server by this secure control channel. If the system has established a user as authorized, the policy settings enable the connection to be established.

- **No new interface to learn.** The Copiun software was designed to be seamless to end users, and there is no new user interface to learn. Instead, this software is integrated into existing and familiar tools such as Windows Explorer or Windows Search, providing full-text search-based recovery for end users. The software relies on an invisible agent that is activated only when the PC is idle, and therefore, it does not disrupt the user.
- **Centralized management.** Copiun designed the software to enable a single administrator to configure and manage groups of endpoint devices across different functional organizations and sites. Also, the administrator can set central policies for end users and then tailor those policies for different organizations. As an example, marketing groups likely require policies specific to backing up photos and other presentation materials that would not be applicable to finance operations.
- **Universal access from tablets/smartphones.** Copiun enables automatic, secure access to the latest copy of a user's PC data from alternate devices like tablets or smartphones, meeting a growing need for mobile users with multiple endpoint devices.

Security

Copiun's software addresses the following security issues:

- The company reports that data transmitted by the CDM PC Agent and the CDM Server is encrypted using AES 128-bit encryption.
- Layers of security are provided by first creating a unique pair of AES 128-bit keys for each network session between the CDM Server and the CDM PC Agent. The symmetric keys used by the CDM Server for encrypting data are not shared with the CDM PC Agent.
- The CAG ensures a secure backup even when a user is not connected to the corporate environment via a VPN, without opening any incoming firewall ports.
- The CDM Server logs each recovery operation performed on the CDM Server. This helps maintain an audit trail to monitor any unauthorized data access activity.
- CDM allows authorized users to perform a federated search across the PC environment for ediscovery and internal forensics purposes.
- The software has a searchable catalog of laptop data. If a laptop is stolen, a company can quickly determine its exposure by accessing a searchable catalog of the laptop's data.

Challenges

The company does face market challenges, however. Chief among those challenges is its start-up status. The company is not yet highly visible in this market. Further, it will be competing with long-established and much larger players.

As a result, the company will face stiff competition that needs to be offset by more than a technology story. Copiun would benefit from adding to its customer success stories.

In addition, the Copiun software, while promising, is positioned as patent-pending technology, which can be concerning to buyers. The company notes that it is in the final stages of the patent process and expects a patent to be granted soon.

Conclusion

Companies are vulnerable to a host of business problems because they do not have a handle on their PC backups. IDC believes that now is the time for companies to be considering backup and data management solutions that anticipate significant changes to the business computing workforce.

Organizations considering adopting new software to improve their backup strategy should take the following steps:

- Determine if there is a requirement for a more centralized approach and assess options on the market that highlight administration capabilities.
- Determine what the technology requirements will be as the environment becomes increasingly distributed and populated by mobile devices.
- Evaluate the need for newer technologies that promise cost savings by delivering more efficient backups in a distributed environment. As an example, object deduplication methods could significantly reduce network traffic by backing up only new data.
- Consider how a software solution addresses the fact that users are increasingly logging into the corporate network on an occasional basis. The software needs to provide backup routines that accommodate these users and should have a particular emphasis on the security ramifications that this creates.

IDC demand-side research shows that firms deploy PC backup to a large degree because of concerns over potential hardware failure, followed by some form of mandate, either legal or regulatory.

As companies grow in size, legal and regulatory mandates play a much larger role in driving firms to conduct a corporate-led PC backup approach. However, nearly a third of all firms surveyed are still relying upon users to back up data themselves and nearly 14% are not backing up data at all. The bottom line is that 45% of firms are not taking a proactive approach to ensure that PC data is protected in the event of a failure, a disaster, a virus, or another security compromise.

With millions of workers accessing the Internet and corporate information through email, companies are at high risk of a business disaster should data be lost, stolen, or corrupted. IDC believes that storage security will surface this year as a priority because of the increase of mobile devices and the resulting concerns regarding data integrity and safety. This should result in new storage architectures to better address this changing environment. To the extent that Copiun can address the challenges described in this paper, the company has a significant opportunity for success.

ABOUT THIS PUBLICATION

This publication was produced by IDC Go-to-Market Services. The opinion, analysis, and research results presented herein are drawn from more detailed research and analysis independently conducted and published by IDC, unless specific vendor sponsorship is noted. IDC Go-to-Market Services makes IDC content available in a wide range of formats for distribution by various companies. A license to distribute IDC content does not imply endorsement of or opinion about the licensee.

COPYRIGHT AND RESTRICTIONS

Any IDC information or reference to IDC that is to be used in advertising, press releases, or promotional materials requires prior written approval from IDC. For permission requests, contact the GMS information line at 508-988-7610 or gms@idc.com. Translation and/or localization of this document requires an additional license from IDC.

For more information on IDC, visit www.idc.com. For more information on IDC GMS, visit www.idc.com/gms.

Global Headquarters: 5 Speen Street Framingham, MA 01701 USA P.508.872.8200 F.508.935.4015 www.idc.com