Business white paper

CIO survey: All's not well at endpoints

HP Autonomy's eDiscovery market offering

Table of contents

With compliance requirements and external threats on the rise, no business can afford to leave its data unprotected, especially at the endpoint. Fortunately, today's IT leaders understand the risk: Fifty-nine percent of recent IDG survey respondents rate backup and protection of desktop and laptop data as crucial or high priority. But even though the majority of survey respondents have something in place, many fall short in terms of meeting needs for identification, classification and discovery.

As a result, these firms—especially those in highly regulated industries—leave themselves in a position of vulnerability. Even though proper protection consumes time and resources, CIOs cannot deny that endpoint information is a potential liability. The big question is, where does a CIO find a non-intrusive way to protect and classify endpoint data to minimize risk that also makes sense economically?

New research shows that although CIOs understand the importance of securing their data, they often fall short when it comes to adequately identifying, classifying, and backing-up.

Understanding the need

The good news is that senior IT executives are clear about the critical need for automating the backup process, according to a recent survey conducted by IDG Research Services. Sixty-six percent of survey respondents consider it a critical or very important objective to provide evidence and audit trails to prove compliance. IDG's research shows that although CIOs understand the importance of securing their data, they often fall short when it comes to adequately identifying, classifying, and backing up data.

A few other key results of the *CIO Survey: All's not well at endpoints* include:

- Sixty-one percent of respondents currently using or planning to use a desktop and laptop backup solution consider improving the accessibility and availability of user data a critical or very important objective.
- Fifty percent of respondents rate the ability to quickly find endpoint data for discovery and compliance purposes a critical or high priority.
- Forty-seven percent of respondents expect an improvement in the ability to improve compliance with industry and government regulations as a result of the efforts their companies are making to effectively backup, protect and manage endpoint data.

According to Jackie Su, Director, Product Marketing for Data Protection at HP Autonomy, there are two key drivers bringing about this increased awareness:

1. Providing much-needed data accessibility and support to mobile employees who count on mobile data while on the go.

2. Protecting the company against the liabilities associated with people carrying this data.

Endpoint asset

While IT has long struggled to effectively support its road warriors, the issue has compounded in recent years, with more workers demanding mobile support. Employees at all levels and across all industries are creating and carrying unprecedented levels of confidential corporate and client information on a wide array of laptops, smartphones, tablets, or other devices.

Today's workforce has grown accustomed to working anywhere, anytime, and on any device. Consequently, not having instant access to this data when needed can have an impact on productivity and the ability to serve the customer base. Imagine, for instance, if an executive loses a valuable presentation from an endpoint device just prior to a scheduled meeting. This does not have to be catastrophic—assuming the IT department views endpoint data as an asset and provides protection. With data available from a secure Web portal from anywhere around the globe, it is possible to retrieve the backup and continue with the meeting unscathed.

Endpoint liability

It's easy to see the benefits of empowering the workforce with robust real-time information. On the flipside, providing widespread access to corporate and client data also represents a significant liability, especially in litigation-intensive industries. As remote data levels increase, IT's ability to accurately and efficiently comply with discovery requests compounds. As data

creation shifts to mobile devices, the process is far more involved. After all, data now goes well beyond emails and server databases.

In addition, there is a limited amount of time to satisfy a discovery request. As a result, the longer an organization devotes to the often tedious task of tracking down and collecting pertinent data, the less time its team has to review and produce an optimal outcome either through trial or settlement. As e-discovery becomes more of an understood risk, companies will see the importance of looking for ways to mitigate cost and streamline information management.

While IT has long struggled to effectively support its road warriors, the issue has compounded in recent years with more workers demanding mobile support.

"The unfortunate reality is that IT has little control over employees' actions. Take for instance, the common practice of utilizing unapproved mobile devices to access, create and store corporate data," says Su. "For IT not to have coverage, the risk of not being able to get a hold of information needed for litigation purposes is higher and higher."

Understanding the gap

Even though IT leaders say they understand the significance of protecting the endpoint, significant data gaps still exist. Specifically, 43 percent of the IDG survey respondents rate their IT organization's current level of visibility as less than adequate. This is alarming when you consider that the purpose of protecting the endpoint goes well beyond availability to include discovery and compliance. According to Su, even though protecting the endpoint has been a priority for a number of years, IT budgets across the board are lean—meaning limited funds quickly dry up as firms address the laundry list of high-priority issues or concerns.

"Part of the justification in allowing endpoint protection to slide has always been the perception that whatever is truly important is probably already backed up through servers, fileshares, or stored within the user's email," says Su. This sentiment was echoed in discussions in a LinkedIn forum recently, when a participant said his organization does not back up endpoint data. "Instead, we opt for a process that instructs users to save data to the network," he says. "There are obvious downsides to this, but all users are aware of the risks: Store the data locally and you have a better chance of losing it."

Effectively closing this gap means CIOs need to go beyond simply accepting that endpoint data is both an asset and a liability to their organizations, explains Su. "This level of endpoint data creation is only going to increase as technologies continue to simplify mobility. Businesses need to take action and find a balance between accessibility and security, properly protecting mobile corporate data, and not hindering employee productivity at the same time."

Roadmap to success

According to CIO Magazine's *2011 State of the CIO*, 89 percent of CIOs expect security strategy and risk management to be a big part of their job within the next few years. This means CIOs need to be proactive in arming themselves with visibility, accessibility, and control over endpoint data for recovery, e-discovery, regulatory compliance, and audits.

When seeking solutions, it is important to first assess the policies in place to protect data at the endpoint. With today's plethora of data on endpoint devices, policies need to go beyond providing IT with the ability to simply secure data. IT leaders need policies in place to allow the fulfillment of legal discovery. With 65 percent of survey respondents voicing concerns about their companies' ability to quickly provide endpoint data to fulfill litigation or audit-based discovery requests, CIOs cannot afford for to wait for an incident to realize protection is inadequate. While it's possible only a small percentage of employees host business-related data on their devices, IT needs a way of accurately discovering data across the enterprise without undergoing a manual exploration. The next step is to review regional and industry-specific compliance requirements in conjunction with the organization's legal department. Taking this step is crucial in accurately establishing a roadmap to address corporate data.

In addition to gaining an understanding of compliance requirements, it is also important to get a grip on specific risks facing the organization. "When you understand the risks you can form a view about the suitability of your countermeasures. You also need to remember that security

is a moving target, and you always need to adapt and invest— it's not like deciding whether to improve a business process or other IT system," says another LinkedIn forum respondent. "Security safeguards against changing threats. It's not about investing to take advantage of opportunities, so there's no choice about continuous investment, and 'good enough' might be different tomorrow. It's also a broad church, covering employee terms, governance, technology, process, communication, and review."

As IT leaders evaluate backup and protection solutions, Su recommends considering a few key aspects:

- It is crucial to embrace an integrated tool capable of providing visibility, accessibility, and control over endpoint data for recovery, e-discovery, regulatory compliance and audits.
- This tool should ultimately simplify the collection of endpoint data for legal holds. It needs to be a defensible, forensics sound, endpoint content collection tool.
- It needs to provide the least intrusive possible way to capture the most information from your users' end-points.
- It must eliminate or at least reduce the cost of over-preservation with surgically precise data collection.

"The unfortunate reality is that IT has little control over employees' actions."

—Jackie Su, Director, Product Marketing for Data Protection

Understandably, going through the process can be a tall task for many IT department leaders who are already stretched thin with increasing levels of responsibility. To ease the burden, CIOs should seek assistance from vendors and consultants who truly understand the associated costs, applications and risks. "Look for a trusted partner who can guide you through the selection process and helps you make crucial decisions—and also understands how to implement a sensible solution for your circumstances," says Su.

Focus on eDiscovery

HP Autonomy offers a proven solution to backup, classify, and collect data for discovery, litigation, and audit requests. Known as the Connected eDiscovery edition, it helps IT leaders to automatically back up crucial endpoint data and gain visibility and accessibility. "Enterprises are facing increasing amounts of litigation, regulatory, and compliance pressures and are bogged down by growing volumes of electronic data," said Vivian Tero, program manager for GRC infrastructure at IDC. "PC backup solutions should no longer simply store and protect data, but also enable the search, collection, and classification of data to seamlessly integrate with e-discovery tools and processes actions."

About HP Autonomy

HP Autonomy is a global leader in software that processes human information, or unstructured data, including social media, email, video, audio, text, and web pages. Autonomy's powerful management and analytic tools for structured information together with its ability to extract meaning in real time from all forms of information, regardless of format, is a powerful tool for companies seeking to get the most out of their data. HP Autonomy's product portfolio helps power companies through enterprise search analytics, business process management and OEM operations. HP Autonomy also offers information governance solutions in areas such as eDiscovery, content management and compliance, as well as marketing solutions that help companies grow revenue, such as web content management, online marketing optimization and rich media management.

Please visit **autonomy.com** to find out more.

Sign up for updates
hp.com/go/getupdated

20130305_RL_WP_HP_AUT_CIO_survey