Avoiding The Hidden Costs of the Cloud

2013

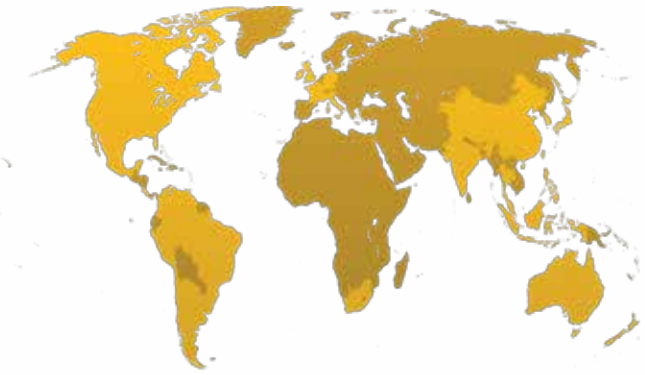
Symantec

CONTENTS

METHODOLOGY

Symantec commissioned ReRez Research to conduct the 2013 Avoiding the Hidden Costs of Cloud Survey in September and October of 2012. They contacted business and IT executives at 3,236 organizations in 29 countries. Respondents came from companies with a range of 5 to more than 5,000 employees. Of the responses, 1,358 came fromSMBs and 1,878 came from Enterprises.

The survey has a reliability of 95 percent with +/- 1.8 percent margin of error.



3,236 global organizations

29 countries

North America *(2 countries)*

United States	102
Canada	100

Latin America *(9 countries)*

Mexico	110
Brazil	102
OLAM	100

EMEA *(5 countries)*

United Kingdom	204
Germany	201
France	202
Italy	201
South Africa	101

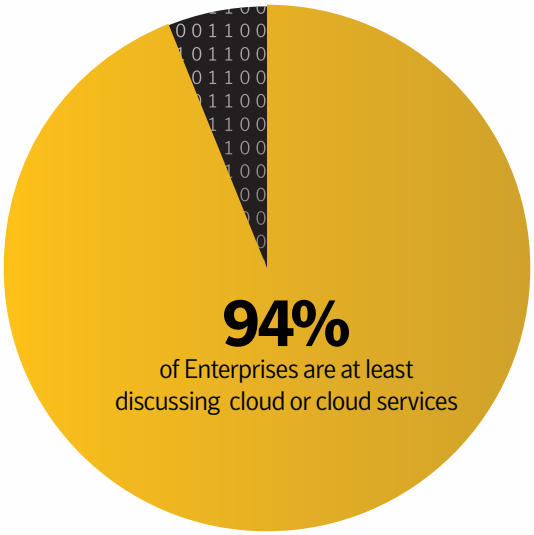
APJ *(13 countries)*

China	204
Japan	301
Australia/New Zealand	200
India	201
Singapore	150
South Korea	100
Hong Kong	103
Malaysia	150
Taiwan	103
Thailand	100
Philippines	101
Indonesia	100

INTRODUCTION

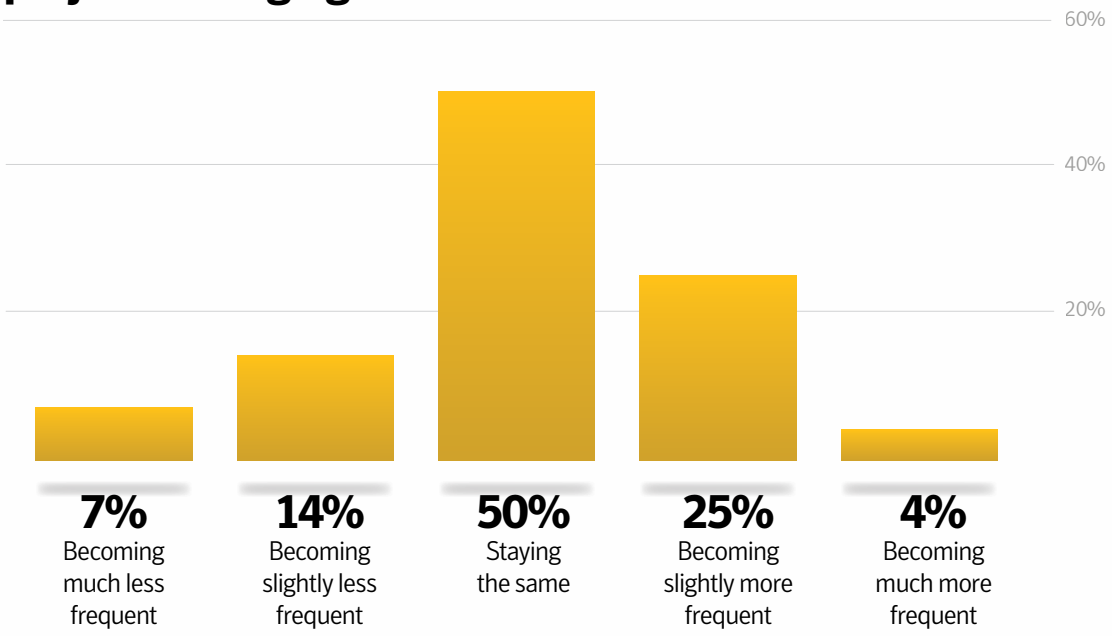
The votes are in, and organizations of all sizes are moving ahead with cloud implementations. The promise of reduced CapEx, more predictable OpEx, easier management, enhanced scalability and better disaster preparedness have made the decision an easy one. In Symantec's 2013 Avoiding the Hidden Costs of the Cloud survey we found that more than 90 percent of all organizations are at least discussing cloud, up from 75 percent a year ago.

However, in a rush to implement cloud, there are a host of hidden costs unwary organizations may face. These costs are easily avoided with a little foresight and planning, but only if IT knows where to look.



ROGUE CLOUD IMPLEMENTATIONS

How is the frequency of rogue cloud projects changing over time:



The first hidden cost Symantec found was rogue cloud deployments. Perhaps the sales manager signs his department up for Salesforce without thinking to consult IT. Or perhaps marketing shares important launch materials with outside vendors via an unauthorized Dropbox account.

In either case the organization has put sensitive information into the cloud without organizational oversight. It's a surprisingly common problem, found in three-quarters of all organizations. It also seems to be an issue experienced more by enterprises (83 percent) than SMBs (70 percent).

Among those who reported rogue cloud deployments, 40 percent experienced the exposure of confidential information, and more than a quarter faced account takeover issues, defacement of Web properties, or stolen goods or services.

So why are organizations doing it? One in five don't realize they shouldn't. However, the most commonly cited reason for these rogue cloud projects was to save time and money: Going through IT would make the process more difficult.

CLOUD BACKUP AND RECOVERY

Today, organizations often store their information on physical, virtual and cloud storage. This can create a very complicated environment when it comes to backup and recovery. In fact, more than two-thirds of enterprises today are using three or more solutions to back up their data.

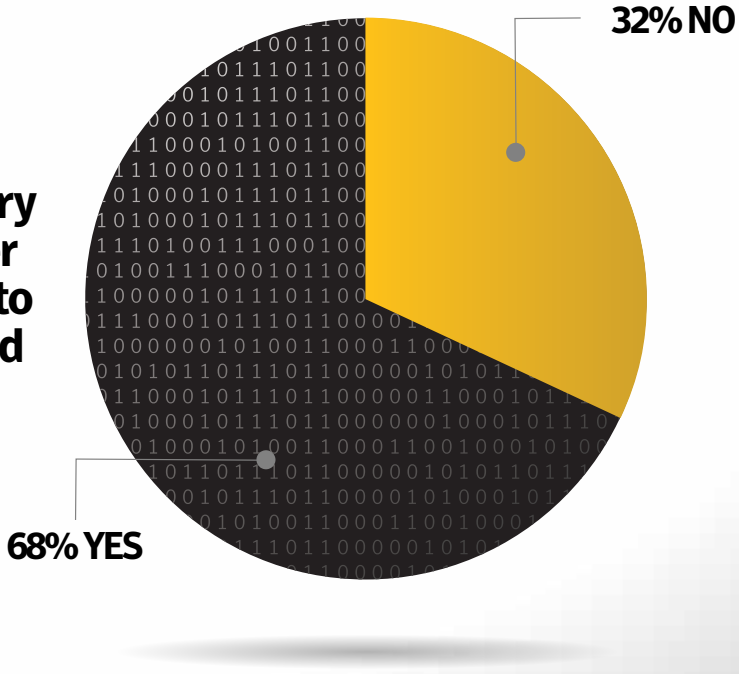
This creates problems for IT, which has to train staff on multiple products and spend extra cycles managing the process. It also means there is no single view of the network. The consequences of this complexity are starting to show.

More than 40 percent have lost data in the cloud and have had to restore their information from backups (47 percent of enterprises and 37 percent of SMBs). Two-thirds of those organizations saw recovery operations fail.

Furthermore, recovering data from the cloud is slow. Just one third rate cloud data recovery as fast. How slow? More than one-fifth estimate recovering from the cloud would take three days or longer.

How many businesses can afford to shut down for three days?

Have you ever had a recovery failure in the cloud? In other words, have you ever tried to restore lost data only to find your backup or archive did not work?



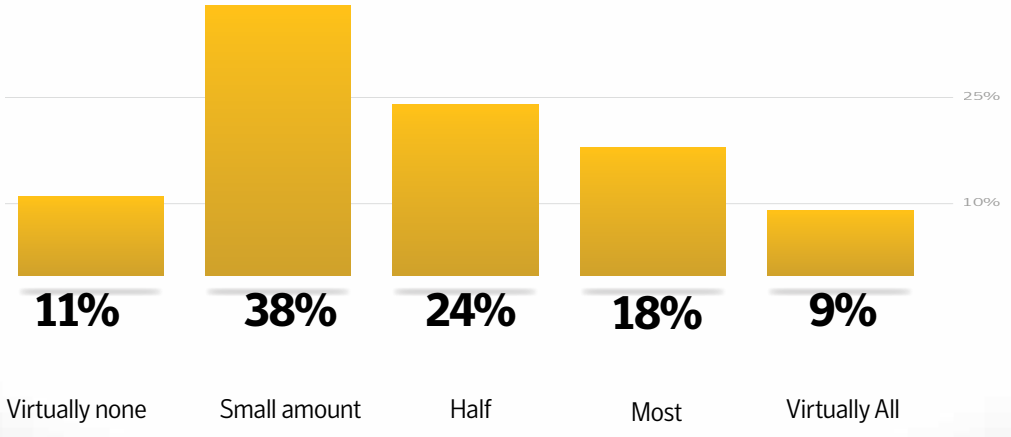
INEFFICIENT STORAGE

Cloud storage supplies important advantages: It is quick to deploy, you pay only for what you use, and you can adjust capacity quickly and easily. In theory, then, organizations should enjoy very high storage utilization rates (this is the measure of the percentage of deployed storage they actually are using). There is no point to over-provisioning since you can always get more storage as you need it with a few mouse clicks.

In practice, however, cloud storage utilization is actually extremely low at just 17 percent. There is a tremendous difference in this area between enterprises (which are utilizing 26 percent of their storage) and SMBs (which is a shockingly low 7 percent). This is a costly mistake, as organizations are paying for roughly 6 times as much storage as they actually need. The problem is exacerbated because half admit that little to none of their data is deduplicated.

Looking deeper, we see challenges tiering data stored in the cloud. Whereas with physical and virtual storage organizations move data among tiers to balance needs in the most efficient manner, many (roughly a third) organizations report moving files in a cloud environment is cumbersome.

What is the status of the data you store in the cloud in terms of duplication:



COMPLIANCE AND eDISCOVERY

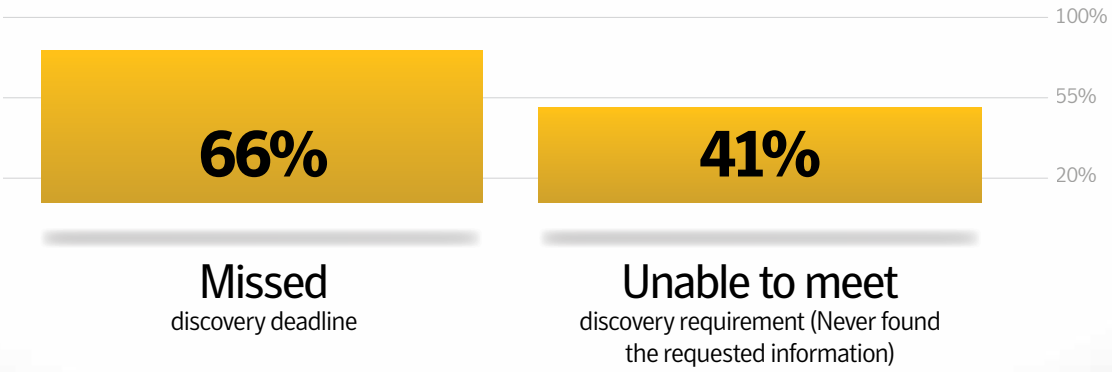
34% have had eDiscovery requests for cloud data

Another hidden cost is compliance. Often, IT has their hands full with simply provisioning and maintaining cloud. A common refrain is that "second order" issues such as compliance can wait. This is a mistake. In fact, 23 percent of organizations have been fined for privacy violations in the cloud within the past 12 months.

Smart organizations know this: Roughly half today are saying they are concerned about meeting compliance requirements in the cloud. Interestingly, simply meeting compliance requirements is not enough; an even larger percentage say they worry about being able to prove their compliance.

The issue of eDiscovery is similar to compliance – an area often overlooked in initial cloud deployments. However, one-third of those surveyed have received eDiscovery requests for cloud information in the past 12 months.

Underscoring the importance of planning for eDiscovery from day one, two-thirds of those who have received requests missed deadlines for delivering the requested information, potentially leading to fines or compromised legal positions.



SSL CERTIFICATE MANAGEMENT

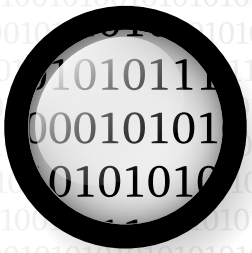
Cloud often requires SSL certificates – for websites, applications, and so on. The final hidden cost revealed by the survey relates to management of these certificates. Most find this area complex: In fact, just 27 percent feel managing cloud-based SSL certificates is easy.

In a related finding, fewer than half feel confident that their cloud partner's certificates comply with their own organization's internal standards.

Only **27%** Say managing SSL certificates related to cloud is easy

Only **40%** are sure cloud-partner's certificates comply with internal standards

AVOIDING THE HIDDEN COSTS



Most organizations are pursuing cloud, and rightly so: Adopting cloud provides clear benefits. The Symantec 2013 Avoiding the Hidden Costs of the Cloud survey shows that as organizations proceed, they need to pay attention to hidden costs of cloud from day one, or else face costly consequences.

Happily, there are simple steps IT can take to avoid these hidden costs.

1. **Focus policies on information and people,** *not technologies or platforms*
2. **Educate, monitor and enforce policies**
3. **Embrace tools that are platform agnostic**
4. **Deduplicate data in the cloud**