# Security, biggest deterrent to storing data in the cloud

**DUBAI:** Security is the number one concern amongst senior business executives when it comes to cloud data adoption, yet more than half of business-critical data is likely to reside there by 2019. According to the findings of a new study released yesterday, by Teradata (NYSE: TDC), the leading data and analytics company, eight out of ten executives cite security as a concern when storing data in the cloud, but that has not stopped a huge rise in the amount of critical data being sent there. Looking ahead to 2019, executives predict that over half of IT (56 percent), customer (53 percent), and financial data (51 percent) will reside in the cloud.

The study highlights that although businesses want to invest in cloud storage and many plan to do so over the next two years, there are real concerns about security of information and data breaches. A number of key trends were identified: Security and lack of control are the top obstacles holding back storage of critical data in the cloud: 40 percent of respondents say general security is a risk, while 25 percent of respondents believe cloud data adoption will result in more security breaches.

A quarter of those surveyed believe data cloud adoption will result in lack of control. 52 percent say executive buy-in to data in the cloud is holding them back and 22 percent struggle with the additional staffing needed to move to the cloud. Yet cloud storage is set to rise sharply in the next two years: Although 58 percent of data from organizations surveyed already sits in the cloud today, usage of cloud will increase over the next two years, with three in ten companies globally predicting a significant increase of data in the cloud by 2019.

**Marc Clark**

Majority of legal data is being held back from the cloud: Legal data is being kept on physical servers for the most part, with just 27 percent of businesses surveyed expecting to move their legal data to the cloud in the next two years. Telecoms are making the biggest commitment to the cloud, with marcomms making strong moves within organizations: 48 percent of organizations surveyed anticipate a significant increase intheir cloud storage use by 2019.

48 percent of marketing and communications departments within organizations surveyed will increase data stored in the cloud by 2019. Healthcare will move its customer data to the cloud, whilst utilities will prioritize IT and R&D data: 59 percent of respondents highlighted that thehealthcare industry will move customer data to the cloud in the next two years. Utilities will prioritize moving IT infrastructure (64 percent) and R&D/Engineering data (52 percent).

Marc Clark, ″Director of Cloud Strategy and Deployment at Teradata said: "Our message to organizations around the world is that the cloud is actually one of the most secure means of virtual storage available. While our study finds widespread concerns, the fact is that cloud storage is growing rapidly, remains hugely cost-effective, and that there are ways to manage it securely.

"Cloud computing security processes should be designed to address the security controls that the cloud provider will incorporate, in order to maintain the data security, privacy and compliance with necessary regulations, as well as providing a business continuity and data backup plan. "By identifying the barriers within the business that hinder further adoption, as well as where cloud storage is creating positive opportunities, we aim to provide reassurance that cloud storage is a safe and cost effective way to store company information."

# With smartphones, customers are corporate whistleblowers

## Smartphones and social media shifts power to consumers

**NEW YORK:** Look out, Corporate America. Customers armed with smartphones and video cameras are watching when you screw up. The viral video of a ticketed passenger dragged forcefully off a United flight is only the latest example of bad behavior exposed in the age of social media. In February, Uber came under fire after a driver posted video of CEO Travis Kalanick berating him.

Earlier, a Comcast technician was shown in a video sleeping on a customer's couch, and an audio recording chronicled one man's herculean efforts to drop Comcast service; they are among the embarrassing customer complaints that ultimately forced improvements. FedEx had to respond after video showed a driver carelessly throwing a package with a computer monitor over the front gate.

Beyond the corporate sphere, smartphone videos of police brutality have prompted protests and investigations. Not long ago, such incidents might have gotten a mention on the local news at most, and quickly disappeared. But smartphone cameras and social media have democratized information and shifted power to consumers. Companies can no longer sweep complaints under the rug.

"That's something a lot of companies just don't get," said Paul Argenti, a professor of corporate communications at Dartmouth's Tuck School of Business. "Companies still operate as if they can hide things and make believe something didn't happen."


**NEW YORK: In this file photo, United Airlines CEO Oscar Munoz speaks in New York, during a presentation of the carrier's new Polaris service. —AP**

### Rewriting the playbook

Companies can't eliminate embarrassing gaffes entirely, but can learn from past blunders to minimize the damage. It starts with training. Employees need to be ready to react when a situation gets dramatic - and companies should emphasize that anything employees do could be recorded. That's especially true for transportation, fast-food and other companies with a lot of employees who interact directly with large numbers of customers.

Running through hypothetical scenarios helps. "Have a couple things planned, what we should do if 'x' happens and what we should do if 'y' happens," said Lakshman Krishnamurthi, a Kellogg School of Management marketing professor. On-site employees need to be given more power to respond to avoid escalating an incident, especially one that might be recorded.

In United's case, for instance, even if employees were following the rules for seeking volunteers to give up seats, they should have been able to read the situation and increase the financial incentives for volunteers rather than drag a passenger off a flight. "You need rules, but you need to be flexible and adapt," Argenti said.

### Block and tackle

Once a video is out there, the standard PR-crisis response remains the same as it always has: Work swiftly to correct the situation in the eyes of the public. "Apologize, talk about why it happened, and say it will never happen again," Argenti said. United CEO Oscar Munoz eventually apologized, but not for two days and after first blaming the customer and airport security. And once a video goes viral, companies have to cede control of the narrative.

"When the video is out there, don't try to countermand what the video says," said Herman Leonard, a professor of business administration at Harvard. In the past, companies had hours or days to respond to a crisis. Now, companies must respond immediately, before a scandal spins out of control on social media. For example, when Domino's Pizza employees posted a YouTube video of workers defacing sandwiches in 2009, the employees were quickly fired, the store was inspected and the CEO apologized. That helped mitigate some, if not all of the damage. —AP

# Facebook looking at behavior to weed out fake accounts

**SAN FRANCISCO:** Facebook on Wednesday said it has started weeding out bogus accounts by watching for suspicious behavior such as repetitive posts or torrents of messages. The security improvement was described as being part of a broader effort to rid the leading social network of hoaxes, misinformation, and fake news by making sure people are who they claim to be.

"We've found that when people represent themselves on Facebook the same way they do in real life, they act responsibly," Shabnam Shaik of the Facebook protect and care team said in a blog post. "Fake accounts don't follow this pattern, and are closely related to the creation and spread of spam." Accounts suspected of being bogus are suspended and holders asked to verify identifies, which scammers typically don't do, according to the California-based social network. In France, the new tactic has already resulted in Facebook taking action against 30,000 accounts believed to be fakes, Shaik said. "We've made improvements to recognize these inauthentic accounts more easily by identifying patterns of activity-without assessing the content itself," Shaik said. —AFP

# CIA chief calls WikiLeaks a hostile intelligence service

**WASHINGTON:** CIA Director Mike Pompeo on Thursday called WikiLeaks a non-state "hostile intelligence service" often abetted by state actors, such as Russia during last year's presidential campaign. "WikiLeaks walks like a hostile intelligence service and talks like a hostile intelligence service," Pompeo told an audience at a Washington think tank.

Russia's GRU intelligence service had used the anti-secrecy group to distribute hacked material during the 2016 US presidential election, he said. WikiLeaks released Democratic emails during the 2016 presidential campaign that US intelligence agencies say were hacked by Russia to try to tilt the election against Democratic candidate Hillary Clinton in favor of Republican Donald Trump, the eventual winner.

WikiLeaks founder Julian Assange said the release was not intended to influence the election. In March, WikiLeaks published documents describing secret Central Intelligence Agency hacking tools and snippets of computer code, but did not publish the full programs that would be needed to conduct cyber exploits against phones, computers and internet-connected televisions. Intelligence and law enforcement officials said contractors likely breached security and handed the documents to WikiLeaks. —Reuters