# IT security problems shift as data moves to 'cloud'

June 24 2012, by Rob Lever


A "Secure Cloud Storage" drive is pictured at the CeBIT, the world's biggest IT fair, in 2011 in Hanover, central Germany. The Internet "cloud" has become the hottest topic in computing, but the trend has created a new range of security issues that need to be addressed.

The Internet "cloud" has become the hottest topic in computing, but the trend has created a new range of security issues that need to be addressed.

The cloud is associated with things like personal emails and music which can be accessed on computers and a range of mobile devices.

But the US military and government agencies from the CIA to the Federal Aviation Administration also use cloud systems to allow data to be accessed anywhere in the world and save money -- and, ostensibly, to enhance security.

Microsoft, Google, Amazon and others are major players in the cloud, which seeks to transfer some of the data storage issues to more sophisticated data centers. Firms like Oracle, SAP and Salesforce.com offer cloud services for business.

Strategy Analytics forecasts US spending on cloud services to grow from $31 billion in 2011 to $82 billion by 2016.

But some experts say security implications of the cloud have not been fully analyzed, and that the cloud may open up new vulnerabilities and problems.

"If past is prologue I don't think any system is absolutely secure," said Stelios Sidiroglou-Douskos, a research scientist at the Massachusetts Institute of Technology's Computer Science and Artificial Intelligence Laboratory.

"The analogy most people give is having a lock on your door. It's not a guarantee no one will break in, but it's a question of how much time it will take, and if your lock is better than your neighbor's."

In a cloud environment, "this makes the job of the attacker so much harder, which means the amateur hacker might be obsolete," said Sidiroglou-Douskos, who is working on a US government-funded research project to develop "self-healing" clouds.

## POTENTIAL GOLD MINE FOR CYBERCRIMINALS

But if a system is breached, analysts say, the amount of information lost could be far greater than what is in a single computer or cluster.

"You can have better defenses" in the cloud, "but if an attack happens, it's highly amplified," says Sidiroglou-Douskos.

The four-year MIT project funded by the Defense Advanced Research Projects Agency seeks to develop systems that automatically fix data breaches in a manner similar to "human immunology," says the researcher.

A number of cloud security breaches have raised concerns, including attacks on the Sony PlayStation Network, LinkedIn and Google's Gmail service. One hacker recently claimed to have stolen credit card numbers from 79 major banks.

"Crimes target sources of value. Large company networks offer more targets to hackers," says Nir Kshetri, a professor of economics who studies cybercrime at the University of North Carolina at Greensboro.

"Information stored in clouds is a potential gold mine for cybercriminals."

Kshetri said in a paper submitted to the journal Telecommunications Policy that when questions come up, "the cloud industry's response has been: Clouds are more secure than whatever you're using now. But many users do not agree."

**'FAKE CLOUDS'**

Marcus Sachs, former director of the Sans Technology Institute's Internet Storm Center, said the cloud may be more secure but also opens up new questions.

"In the cloud, you don't necessarily know where your data sits," Sachs told AFP.

"That doesn't make it less vulnerable to attack, but there are questions when it comes to (an) audit, or if you want to take the data back or

destroy it, how do you know you've erased it?"

Sachs said that analysts have also discovered "fake clouds" which are offered as low-cost alternatives but are in fact operated by "criminal groups which monitor and steal the data."

"We have seen instances of this not in the US, but in the former Soviet Union and in China," he said.

Still, the cloud market is burgeoning, with companies and government agencies moving to either "public" clouds that are easily accessed or so-called "private clouds" that are segregated from the Internet.

Some analysts say other issues need to be resolved about cloud computing, such as who is liable if data is lost, and how data can be accessed for government investigations.

Outages have recently affected Apple's and Amazon's cloud services, causing some websites to be affected.

"Privacy, security and ownership issues in the cloud fall into legally gray areas," Kshetri says.

Sidiroglou-Douskos said there is no single answer for people or companies choosing between cloud systems and holding the data themselves.

"If you are trying to protect yourself from the government, then having it in the public cloud makes it easier for them to get it," he said.

"If your main worry is a hacker in Russia, maybe (cloud) infrastructure is better for your own security."

(c) 2012 AFP