AS MORE ORGANIZATIONS ADOPT THE CLOUD, NEW ISSUES WILL CONTINUE TO EMERGE.

Each issue, IEEE Cloud Computing news briefs looks at recent happenings and trends in the cloud world.

Clouds Leave Corporate Data Vulnerable to Ex-Employees

Even after leaving their jobs, two-thirds of employees who used their companies’ cloud systems could still access data there, according to a recent study.

Also, 25 percent of respondents said they would violate policy by taking business data with them when leaving their companies, according to the survey of 1,000 office workers at companies with at least 3,000 employees in Australia, France, Germany, the Netherlands, the UK, and the US.

About 20 percent of participants admitted that they’d already uploaded proprietary corporate data to a personal cloud application such as Dropbox or Google Docs to share outside of the business.

These findings demonstrate the security problems that cloud technology poses for many companies and help explain why many organizations have chosen not to use the cloud for important data or applications.

Market research firm Vanson Bourne conducted the survey for identity- and access-management provider SailPoint.

“The survey results are an eye opener of how cloud applications have made it easy for employees to take information with them when they leave a company,” said SailPoint president Kevin Cunningham.

The survey identified other issues in finding that only 28 percent of respondents stated their employers’ policies even address who has access to mission-critical cloud-based apps, and 20 percent said they acquired a cloud application for work without informing their IT departments.

Because of this, Cunningham added, “It’s virtually impossible to manage access to applications and the sharing of mission-critical data. In order to establish control over this bring-your-own-app phenomenon, it’s critical to provide specific incentives for end users to follow corporate policy such as offering users a seamless login experience in exchange for using a central access control framework.”

However, experts say, solving the cloud-security problem will require more than this, including user education.

Cloud Computing Could Save Energy, Reduce Harmful Gas Emissions

Cloud-computing use could help cut global greenhouse-gas emissions, reduce global dependence on nonrenewable energy sources, and save users $2.2 billion in energy costs, according to a recent study.

Researchers from Harvard University, Imperial College, and Reading University compiled the Enabling Technologies of a Low-Carbon Economy—a Focus on Cloud Computing report.

It was based on a survey—sponsored by Microsoft Europe and the Global e-Sustainability Initiative (GeSI)—conducted in Brazil, Canada, China, the Czech Republic, France, Germany, Indonesia, Poland, Portugal, Sweden, and the UK. GeSI promotes environmental sustainability in the IT and communications industries.

The research studied ways that implementing cloud-based services could reduce energy usage and pollution.

Using the cloud could reduce power consumption and emissions because organizations wouldn’t have to run the on-site servers and other equipment they now need to provide services in-house, according to the report. This, in turn, would save energy by reducing the amount of equipment that hardware vendors must manufacture.

The new study said that if 80 percent of private and public organizations employed cloud-based email, customer relationship management (CRM), and groupware technology, they could decrease annual global power usage by an
amount equivalent to 75 percent of the energy consumed in the Brussels area and 25 percent of that used in London, and would have the same effect as removing 1.7 million cars from the streets.

However, the researchers cautioned, the actual degree of benefit will depend on how many organizations adopt cloud computing and the extent to which they use it.

In 2013, the US Lawrence Berkeley National Laboratory’s Computational Research Division and the Northwestern University McCormick School of Engineering and Applied Science’s Environmental Energy Technologies Division released results of a six-month research project that concluded that adopting cloud approaches could reduce companies’ infrastructure and energy costs.

The study, which Google funded, concluded that if a significant number of US companies used cloud-based CRM, email, and productivity applications, they could save 23 billion kilowatt-hours, enough to provide Los Angeles with one year of electricity.

Get Ready for the Mobile Cloud
Two major trends in business operations have been workers’ increased use of mobile technology and companies’ ongoing implementation of cloud technology.

Industry observers say that the two trends are merging into the mobile cloud and that this approach will soon become considerably more popular.

A recent report by Research and Markets, an industry-analysis firm, forecasts the worldwide mobile cloud market will increase from $9.43 billion last year to $46.90 billion by 2019. This represents a compound annual growth rate of 37.8 percent.

The report said mobile cloud technology is gaining steam mainly because a rapidly growing number of employees are using wireless devices and apps on the job due to their convenience, constant availability, and growing functionality.

Proponents say combining today’s smartphones and tablets with productivity-related mobile apps and hybrid private-public cloud-computing services provides employees with flexibility and options they don’t otherwise have.

In some companies, workers are already acquiring mobile cloud apps to use for purposes such as synchronizing files they generate on their wireless devices with the corporate network.

However, current and potential mobile cloud users still express concern about security, privacy, and available bandwidth.

Survey: Half of Organizations Abandon or Delay their Cloud Migrations
Migrating to the cloud can be difficult, according to a recent study.

About 43 percent of respondents to the survey noted that they had either given up on or delayed their planned cloud implementations.

During the implementation process, half of the respondents said they had budget overruns, 65 percent had to significantly alter their original plans within a year, and 52 percent had to do so in the first six months.

Only 27 percent said they were pleased with their cloud-migration experience.

These are key results—detailed in a report titled The Adventures of Moving to the Cloud—from a survey by cloud-hosting service provider INetU and the THINKStrategies consultancy of 358 organizations that recently undertook migrations.

The study detailed what respondents reported as the most difficult aspects of cloud implementations: security (cited by 27 percent), compliance with legal regulations (20 percent), capacity planning (13 percent), monitoring (9 percent), provisioning (4 percent), and billing (4 percent).

The easiest aspects reported were billing (50 percent), provisioning (34 percent), monitoring (30 percent), compliance (27 percent), security (22 percent), and capacity planning (21 percent).

“Too many organizations moving to the cloud are learning just how complex migrating to the cloud can be and are paying the price with setbacks including project delays, re-engineering, and cost overruns,” said INetU vice president of strategy David Fowler.

The survey report concluded that successful implementations entailed cloud services customized around an organization’s specific needs, a structured migration process, and continuous business and performance management.

It also recommended using a cloud-service provider—which would include a company such as INetU—to manage migrations and implementations.

Researchers Find Critical Flaw in Docker Technology
Security researchers have found a major vulnerability in the increasingly popular open source Docker platform. Docker makes it easier to download applications over the Internet and run them...
on various types of machines via cloud platforms.

Florian Weimer, a member of open source software vendor Red Hat’s Product Security team, and independent security researcher, Taunis Tiigi recently found the flaw in all but Docker’s current version.

In versions up to and including Docker 1.3.1, noted Docker Inc., “this vulnerability could be leveraged to perform remote code execution and privilege escalation,” and ultimately steal files hosted in the cloud.

The company has since released version 1.3.2 to remedy the problem and advises users to download it as soon as possible, as there is no fix for the recently found bug.

The issue is important for cloud users, as major technology companies such as Amazon and Google are supporting Docker.

Developers use Docker to put applications in software containers so that users can download them across the Internet or any private network and then run them on any cloud platform or Linux machine.

This would be a huge benefit for cloud computing, which is typically used to make applications that are kept online available to all types of computing devices.

Proponents add that Docker also makes developers’ lives much easier by letting them focus on designing programs without worrying about the machine or platform on which they will run.

Demand for Hybrid Clouds Will Boost Cloud Market
Corporate demand for hybrid public-private clouds will drive a healthy growth in the overall cloud market, according to industry research firm IDC.

The company predicts that the global cloud market will be worth $118 billion in 2015—23.2 percent more than 2014’s $95.8 billion, which was 25.9 percent more than 2013’s $76.1 billion—and reach $200 billion by 2018.

IDC says that the hybrid approach is helping to spur adoption by letting companies combine a private cloud’s security with a public offering’s low cost. This provides businesses with a safe starting point for their cloud experimentation and implementations. Not many organizations are using the hybrid cloud for mission-critical tasks yet.

Industry-analysis firm Technology Business Research (TBR) forecasts growth of 35 percent in the private-cloud market and 25 percent in public-cloud adoption, but 50 percent in hybrid cloud implementation from 2014 to 2015.

Like IDC, TBR says the hybrid market’s growth will be due to companies wanting to begin their cloud adoption with a more cautious approach.

Another factor increasing cloud adoption, according to IDC, is increasing user confidence in the cloud’s security and reliability, although security concerns continue to cause some companies to shy away from the technology.

The Solution to the Security-Employee Shortage Is in the Cloud
One of the important technology themes of 2014 was the shortage of expert personnel that has plagued companies looking to beef up their cybersecurity staffs.

In its 2014 Annual Security Report, Cisco Systems said there is a global shortfall of 1 million security professionals.

Thus, the study said, most organizations are unable to continuously monitor systems, find intrusions, and eliminate problems, particularly when threats require a sophisticated analysis of network data.

For many of these companies, as well as businesses that can’t afford to hire full-time security staffs, the answer is increasingly in the cloud.

Service providers are beginning to provide various types of sophisticated security monitoring and an analysis of the resulting data to recognize problems, all via the cloud. Other vendors combine system monitoring with a cloud-based platform that collects information from customers and threat-intelligence reports to identify intrusions and other threats.

These services—offered by providers such as CrowdStrike, Cyphort, and FireEye—reduce the number of security employees, hardware, and software companies need to acquire.

Various experts caution that in some cases, the new approach might be less effective than traditional systems in reducing threats because cloud-based security is less aware of the customer’s overall computing environment than in-house implementations.***