COMPUTERWORLD

Subscribe to a Newsletter   Solution Centers ▼   Events   Magazine ▼   🐦 📘 📶 RSS

Google™ Custom Search

| Topics ▼ | News | In Depth | Reviews | Blogs ▼ | Opinion | Shark Tank | IT Jobs | White Papers | Webcasts | More ▼ |

Security

App Security | Business Continuity | Cybercrime and Hacking | DRM and Legal Issues | Data Security | Malware and Vulnerabilities | Privacy | Security Hardware and Software

Home > Security

Cutting though the fog of cloud security

As cloud computing's security gaps become more visible, users are finding ways to safeguard their data.

By John Edwards
February 23, 2009 12:00 PM ET

💬 Add a comment   👍 Like   ➕1 0

Computerworld - Daniel Flax, CIO at New York-based investment banking and financial services firm Cowen and Co., relies on cloud computing to automate his company's sales activities. While he's satisfied with cloud technology's potential to lower upfront costs, decrease downtime and support additional services, he admits that he has had to work hard to get a handle on the emerging technology's security weaknesses. "Security is one of the things we've had to come to grips with," he says.

Evan Jones, owner and IT chief of interactive production company Stitch Media, located in Toronto and Halifax, Nova Scotia, is also concerned about cloud security. "It's a scary concept when you just hand all of your important company data over to a third party," he says.

Like a growing number of IT managers, both Flax and Jones are beginning to realize that cloud computing doesn't offer companies a free ride when it comes to security. A Gartner Inc. report released last year identified concerns about risks in several areas, such as data privacy and integrity and compliance management, that should give pause to anyone thinking about rushing into cloud computing.

"Enterprises, particularly those in regulated industries, need to weigh both the business benefits and risks of cloud computing services," warns Jay Heiser, a Gartner analyst.

One of cloud computing's biggest risks arises from its very nature: It allows data to be sent and stored just about anywhere -- even divided among locations around the world. While data dispersion helps give cloud computing a cost and performance edge, the downside is that business information can land in storage systems in locales where privacy laws are loose or even nonexistent.

Flax, who is using Salesforce.com Inc.'s Force.com platform to automate Cowen's global sales systems, says the best way to ensure that data steers clear of risky destinations is to work with a cloud vendor that is a public company and is therefore required by law to disclose how it manages information.

Salesforce.com is publicly traded, and "as a result, we have a sense of comfort that there are strict processes and guidelines around the management of their data centers," Flax says. "We know our data is in the U.S., and we have a report on the very data centers that we're talking about."

Top Stories

- Phishing scams likely, warns DHS
- Image gallery: Steve Jobs through the years
- Elgan: How Apple will kill cable TV
- Wireless carriers prep for Hurricane Irene

Security White Papers

Move from Paper to Digital Document Capture for Improved Business Processes
Document intensive business processes are costly and often waste paper as well as storage - pushing costs higher. Digitizing these processes can help...

Setting a Strategy for Secure Mobile Printing
HP's mobile printing solutions help employees to print securely and easily no matter if they're on the go, in the office or at...

The Philosophy of Security
Security is often looked at from the perspective of fear, but a holistic approach can prove more effective. This paper explains how to...

Key Data Integrity and Privacy Regulations for Businesses
Information is currency in today's converged world. Safeguarding this valuable asset not only enables business acceleration, it also ensures business continuity. In an...

HIPAA Goes HITECH
Many healthcare organizations think that traditional IT security and compliance are sufficient safety measures for PHI. The truth is 70% of healthcare organizations...

All Security White Papers

Security Webcasts

Seven Emerging Trends in Endpoint Encryption
As breach notification laws began to emerge that offered safe harbor protections for encrypted data, enterprises found a renewed, and urgent, interest in...

Selecting a DDoS Mitigation Provider
Learn how Verisign manages and helps protect the Internet against DDoS attacks. This webinar will also provide you with best practices for business...

Cloud Security and Risk Management
What's TRENDing is a video/podcast series in which recognized information security leaders are interviewed on timely topics and how they solved or were...

Advanced Authentication Methods: Software vs Hardware
Hardware tokens were a popular method of strong authentication in past years but the cumbersome provisioning and distribution tasks, high support requirements and...

Agora Games, a company in Troy, N.Y., that builds Web communities for video game players, currently has no say on the matter of where its cloud computing provider, Terremark Worldwide Inc., hosts its data and applications. But that will be changing in the near future, says Brian Corrigan, Agora's chief technology officer.

Terremark will soon give Agora "the option to choose where virtual machines actually run," he says. "Right now, the only choice is the Miami facility, but Terremark is adding other locations, so [it will be] an issue we can manage however we want."

Track and Trace

Cloud computing's dispersed nature also makes it challenging to track unauthorized activity, even when careful logging procedures are used. Virtually all cloud computing providers use encryption, such as Secure Sockets Layer technology, to safeguard data in transit. But Heiser notes that it's also important to ensure that stored data is encrypted. "If data is stored in a shared environment, which is what usually happens, you can assume that unencrypted data may be read by unauthorized parties," he says.

Mike Mullin, IT director of Indian Harvest Specialtifoods, a Bemidji, Minn.-based company that distributes rice, grains and legumes to restaurants worldwide, says he relies on provider NetSuite Inc. to ensure that the data he sends into the cloud is fully protected. "With SSL, I'm pretty confident that our data is secure," he says. "If it isn't, then I think a lot of people will have problems and that the [cloud] industry as a whole will have a problem."

Mullin notes that cloud adopters also need to closely assess their own infrastructures and security practices, particularly access controls. "Your side of the infrastructure is just as vulnerable, if not more vulnerable, than the provider's side," he says.

5 Steps to Cloud Security

1. Understand the cloud. Realize how the cloud's uniquely loose structure affects the security of data sent into it.

2. Demand transparency. Make certain that the cloud provider can supply detailed information on its security architecture and is willing to accept a security audit.

3. Reinforce internal security. Ensure that internal security technologies and practices, such as network firewalls and user access controls, are strong and can mesh well with cloud security measures.

4. Consider the legal implications. Understand how laws and regulations will affect what you send into the cloud.

5. Pay attention. Look for changes in cloud technologies and practices that may affect your data's security.

| 1 | 2 | Next page ▶ |

Comments (Add a comment)   Print   f Like   +1 0

Additional Resources

WHITE PAPER
Options for Protecting against Web Threats

This independent paper from senior analyst Jon Collins at FreeForm Dynamics considers how Web-based security threats are evolving, within the context of IT trends including mobile, home computing and other forms of remote access that could potentially increase the attack surface of the companies. It defines the scale and types of threat, what to look for in a corporate web security solution and compares the different types of technological approach available to companies and the processes that need to be considered for effective protection.

Read now.

WHITE PAPER
Enter the Security KnowledgeVault

Security is not an option. This KnowledgeVault Series offers professional advice how to be proactive in the fight against cybercrimes and multi-layered security threats; how to adopt a holistic approach to protecting and managing data; and how to hire a qualified security assessor. Make security your Number 1 priority.

Read now.

WHITE PAPER
Guide to SMB Communications

To date, small businesses have been unable to cost justify an IP-based communications system. This paper provides organizations with fewer than 250 employees a way to meet unique voice and data communications needs even with a limited budget and small IT staff.

Read now.

Like

DISQUS

Comments powered by **COMPUTERWORLD**

Our Commenting Network | Policies | Privacy

Add New Comment

Login

Showing 0 comments

Sort by newest first

✉ Subscribe by email   RSS

Partnered Content

2011 Web Security Report

The first few hours of a new Web attack show that traditional defenses lack adequate protection. This 2011 Web security report details how cybercriminals have modified their tactics to successfully

Magic Quadrant for Secure Web Gateway

Web 2.0 and associated malware threats continue to drive the secure Web gateway market. This Gartner Magic Quadrant ranks the key vendors in this market and highlights their product

Corporate Web Security — Market Quadrant 2011

The corporate Web security market has many vendors offering appliances, software, hosted services, and hybrid solutions that help secure and manage Web traffic. This Radicati

Blue Coat®

use the Web as their attack vector and highlights the need for a Web defense layer to evaluate dynamic Web links leading to Web threats.

Download this white paper

differentiators. Read Gartner's opinion on on-premise solutions vs. cloud-based services and discover the vendors that are leading the charge to keep the Web secure.

Download this white paper

Market Quadrant evaluates key features such as malware protection, URL filtering, and data loss prevention and ranks the market leaders according to product functionality and market share.

Download this white paper

▲ **Skip to top**