Executive Series

Security Essentials for CIOs

Educating Everyone to Guard the Cloud

Highlights:

Like other risks, the challenges posed by cloud computing are nothing that education, best practices and good tools cannot handle. At IBM, we use a set of seven security essentials to better guard the cloud.

Most CIOs are all too familiar with the pros and cons of cloud computing. Because of their flexibility, potential cost savings and ease of use, these remote, professionally managed data centers are spreading fast around the world. Yet many potential customers hold back, maybe with good reason. In a recent Ponemon Institute report, over 60% of surveyed US and European cloud service providers said they were unsure if their cloud applications were sufficiently secured. Additionally, a majority of those cloud providers believed it was their customer's responsibility to secure the cloud, not theirs.[1] This could lead customers to wonder whether sensitive files might mingle with other companies' data. They may question how data is backed up, or what happens if the cloud should experience an outage, or if the cloud provider goes out of business?

Those questions, while serious, are dwarfed by the key security challenge facing a CIO in the clouds: the rise of empowered non-IT professionals. Cloud computing hands the controls to hundreds or thousands of well-meaning users throughout the enterprise. This means that folks who formerly were only technology consumers are now given permission to build systems—but often without understanding vulnerabilities that can potentially put the entire enterprise at risk. Traditionally, trained professionals—the CIO's own team—have handled this work. They are schooled in risks and follow best practices for things like systems configuration, software maintenance and access control. In a cloud, though, this inner circle cedes much of its control. The resulting democratization of technology contributes greatly to efficiency and innovation. This newfound power can also cause significant risk, unless and until users truly understand what they're building and how to maintain it.

One important—and often overlooked—solution is education. Creating a secure cloud environment requires a broad company-wide effort to instruct everyone about smart and careful procedures in the cloud. It involves creating a risk-aware culture. For example, a sales professional building a hosted product demonstration for an upcoming client meeting needs to do so in an informed way, following the proper procedures. The same is true for a human resources manager who is setting up a new cloud-delivered performance review application. They must know that a deviation from the rules, from using an unsecured image to sharing or repurposing passwords, can open the gate to attacks and potentially endanger the enterprise. Everyone developing a cloud-delivered service becomes, de facto, an IT architect. All must understand the risk, learn the appropriate lessons and shoulder the responsibilities.

Over 60%

of surveyed US and European cloud service providers were unsure if their cloud applications were sufficiently secured.[1]

Source: Ponemon Institute

These efforts are especially important because the cloud experience can lull unsuspecting users into lowering their guard. For users, a cloud can feel much like commercial services they've grown comfortable with, such as app stores for their smart phones and tablets. Think of the cloud as a far-away town, with its customers occupying houses there. The town may have sensible laws and a diligent police force, but it's up to the home-owners to lock their doors, set up motion detectors and keep the kids from lending out their keys willy-nilly. Even though most clouds are run by seasoned professionals and provide security services, vigilance and common sense from users is also required.

Think of the cloud as a far-away town, with its customers occupying houses there. The town may have sensible laws and a diligent police force, but it's up to the home-owners to lock their doors, set up motion detectors and keep the kids from lending out their keys willy-nilly.

Once a secure environment is in place, the next challenge is to maintain it through time. Conditions change. Cloud users have to be alert for "security drift". For example, the sales professional who is using the cloud for a product demonstration might neglect to download and install the latest software updates for the system, which contain a critical security patch. While this might not impact his immediate need—which is to present the product to his client—it could introduce risks to the rest of the cloud-based environment.

Like other risks, the challenges posed by cloud computing are nothing that education, best practices and good tools cannot handle. At IBM, we use a set of seven security essentials to better guard the cloud:

Security essentials for cloud computing

1. Educate

The cloud distributes much of the traditional work of the IT staff, allowing nearly everyone to access and customize the images they use. Before they start, they must understand the risks and responsibilities, and follow a set of best practices that they understand and respect. Creating a risk-aware culture is crucial for security—and nowhere is this more important than in cloud computing.

[1] "Security of Cloud Computing Providers Study", Ponemon Institute: Research Report, April 2011 (http://www.ca.com/~/media/Files/IndustryResearch/security-of-cloud-computing-providers-final-april-2011.pdf)

2. Protect the data

Encrypt the data. Identify those with access to the data and give each access only to what is needed for his or her job. The IT team should appropriately monitor this activity to help prevent unauthorized people—or even worse, outsiders—from gaining access to back channels.

3. Maintain a secure environment

It's a snap to use images—and dangerously easy to lose control of them, especially in a large cloud. When this happens, they risk falling behind on security patches. Since unpatched software can increase the risk of malware infection and data leakage, it is vital to have a detailed record of each image—and to limit the population to those that are securely configured, necessary, and up-to-date.

4. Never stop testing

The computing tools and environment must be tested both prior to deployment, and afterwards. Vulnerabilities tend to open up over time, which is why validation and assessment is vital. This should include testing to confirm that default passwords are not used and that the network interface doesn't leave doors or windows ajar.

5. Verify the vendor

Do you know and trust the cloud vendor, and do the people there understand and meet and comply with your business needs and requirements, including security requirements? The answers must be yes. And if you part ways with the vendor, what happens to the data? Figure this out at the beginning—not the end.

6. Enforce governance

Even data that's 10,000 miles away must comply with ever-changing governance. Each company must be able to carry out regular audits of its data and generate compliance reports. And if adjustments are needed, the company should be free to carry them out—just as if the data were housed on site.

7. Consider the country

The location of the data center can make a huge difference. In some jurisdictions, a government has rights to data placed within its borders. In some places, political unrest or electrical outages could disrupt data centers. In the end, you're investing not just in the cloud provider, but in a country.

Security essentials for CIOs

At IBM, our approach to finding a balance between innovation and the need to control risk involves a set of essential practices. These provide a path to security intelligence in a hyper-connected era.

How do I securely embrace the cloud?

Balance access and education

Join the conversation

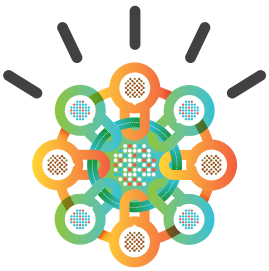
To read additional articles, learn more about Security Essentials for CIOs, or share your thoughts with other security leaders join us at **ibm.com/smarter/cai/security**.

About the author

Kristin Lovejoy is Vice President of IT Risk, Office of the CIO, IBM. She can be contacted at **klovejoy@us.ibm.com**.

About IBM Center for Applied Insights

The IBM Center for Applied Insights integrates deep content and analytical expertise to help chart the course to new value for clients. The Center conducts research and builds assets and tools with pragmatic guidance to provoke organizations to action.



IBM Global Services
Route 100
Somers, NY 10589
U.S.A.

Produced in the United States of America
March 2012

WGW03004-USEN-00