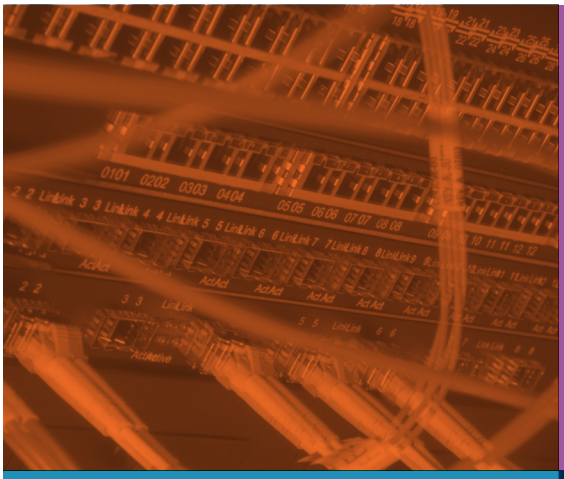
QUICK START GUIDE

Tackling Cloud Security Concerns



A PRACTICAL GUIDE FOR SOLUTION PROVIDERS

CompTIA

Powered by

Cloud COMMUNITY

IT Security COMMUNITY

Introduction

Amazon, Dropbox and Epsilon all made the news in 2011 for security incidents involving their cloud services. CIOs contemplating "what if" scenarios got to see firsthand the results of a significant cloud outage, a password snafu leaving data exposed, and the malicious hacking of a cloud service provider.

Despite the questions these incidents raise, the transition to the cloud computing model continues to accelerate, thanks to the benefits that can be gained in areas such as agility or scalability. More and more companies adopting cloud need to contend with one or more of the many existing and emerging cloud security risks.

Not surprisingly, top of mind security concerns related to cloud computing tend to revolve around system outages and data loss. It's worth keeping in mind that many organizations are still in the experimental stage with cloud computing and may not yet have considered certain risks.

As an IT Services Provider, your interest in cloud security may range from evaluating security provisions as a potential consumer of cloud-based services to assessing the security preparedness of potential partners. Regardless of the role you intend to play, awareness of the questions to either ask or be prepared to answer is key to the success of your cloud-based venture.

TIP #1: KNOW THE CONCERNS

One of the primary technologies supporting cloud computing is virtualization, and it is important to understand how this may cause concern for a security strategy. The creation of virtual machines (VMs) introduces new variables in the security equation. The hypervisor is an extra layer that must be secured, and communications between virtual machines on a single physical server must be monitored, since network tools that observe traffic on physical connections are not useful. In addition, VM sprawl can occur due to the ease of creation and the lack of a process for tracking machines. As security patches for operating systems are released, each VM must be updated. This can be a difficult task if the full set of machines has not been catalogued. The management tools provided by virtualization vendors can assist with the necessary activities to secure a virtual environment, but the most important tools are a proper understanding of the environment and governing policies.

Understanding of the environment and policies of a cloud provider also plays a key role in securing cloud services. The biggest difference between a cloud solution and an on-premise solution is that control has been given to someone else: namely, the cloud provider. It is not sufficient to assume that the cloud provider is adequately securing data and applications. Companies must review how they want to handle security, reliability, compliance, and legal issues related to their cloud service; then they must carefully review the service level agreement (SLA) and discuss security with their cloud provider. Any gaps in the provider's security coverage need to be addressed through changes in policy for the end user.

TIP #2. BUILD ON THE TRUST... BUT QUESTION IT TOO

Despite concerns, most cloud users report being confident or very confident (net 85%) in their cloud service provider's security. A few notable incidents not withstanding, this should be viewed as a testament to the quality of service offered by the major cloud providers and the support provided by IT solution providers.

While confidence in cloud security is high, the level of due diligence reported raises the question of whether that trust is misplaced. According to data uncovered in *CompTIA's 9th Annual Information Security Trends* study, only 3 in 10 customers report engaging in a heavy and comprehensive review of the security policies, procedures, and capabilities of their cloud service provider. In comparison, 44% engage in a moderate level of review, while 13%

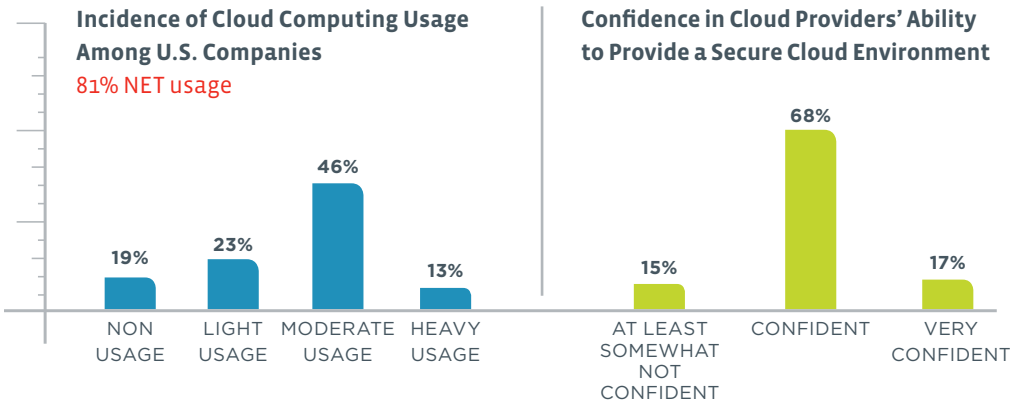
TOP 10 CLOUD SECURITY CONCERNS

1. System downtime/business interruptions
2. Exposure or loss of data during file transfers to the cloud
3. Concerns over encryption of data (either transactional or at rest)
4. Physical security of cloud service provider data centers
5. Shared technology vulnerabilities in a multi-tenant environment
6. Malicious activity from privileged insiders
7. Identifying/authenticating users
8. Difficulty in assessing and comparing the security of cloud service providers
9. Complying with legal/regulatory requirements
10. Ability to conduct audits, review cloud security logs, etc.

Source: CompTIA's 9th Annual Information Security Trends study

Other concerns mentioned in CompTIA research include: loss of control, vendor lock-in, lack of transparency with location of cloud data centers, and insecure APIs.

ORGANIZATIONS GENERALLY CONFIDENT IN CLOUD SECURITY



Source : CompTIA's *9th Annual Information Security Trends* study Base: 500 U.S. Companies

engage in little or no review (14% indicated the review is situational).

That most organizations include at least a moderate level of review is likely viewed by many security mavens as a "cup half full, half empty" situation. On the one hand, given the cloud model is still relatively new to many organizations, it's encouraging to see solid numbers of users evaluating their cloud provider in areas such as encryption policies and disaster recovery plans. On the other hand, many critical elements of the cloud security equation appear to be routinely overlooked, such as regulatory compliance, geolocation of data, and the credentials of the provider.

SMBs in particular, with often lower levels of IT sophistication, may make the assumption that all aspects of security will be sufficiently handled by their cloud service provider, which may or may not be the case. This is confirmed by the data, where only 22% of small firms report engaging in a heavy review of their cloud service provider's security practices, compared to 41% for large firms.

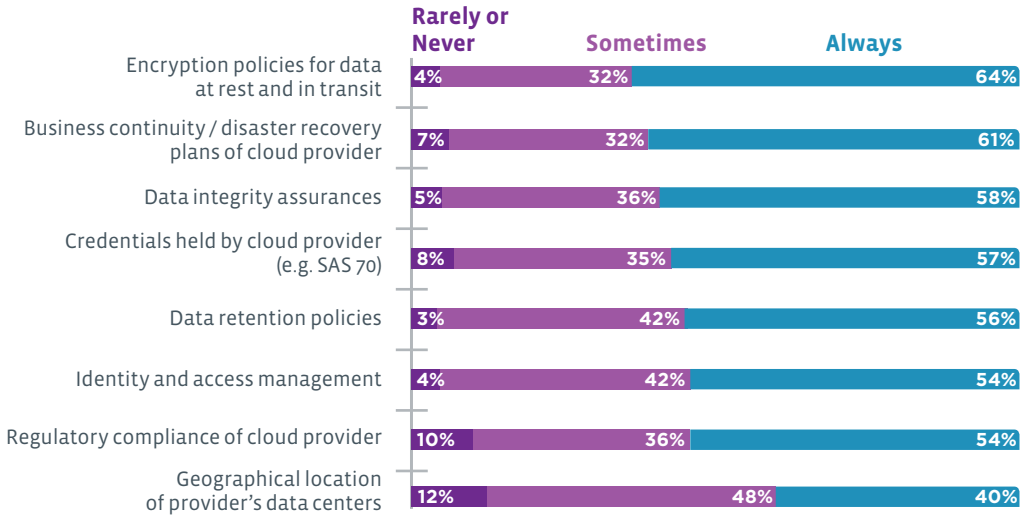
CompTIA's research found that when inquiries are made, questions about the cloud service provider's encryption policies, business continuity and disaster recovery, and data integrity top the list. Areas that are evaluated less frequently, and therefore a potential area of need among customers, include

1. **Data integrity and retention policies,**
2. **Credentials held by cloud service providers (e.g. SAS 70),**
3. **Identity and access management, and**
4. **Regulatory compliance.**

TIP #3. KNOW THAT NOT ALL DATA IS MEANT FOR THE CLOUD…AND THAT'S OKAY

All signs point to even greater levels of cloud adoption in the coming years, but it could be some time before organizations use the cloud for the majority of their systems. According to *CompTIA's 9th Annual Information Security Trends* report, large numbers of organizations have no intention of putting certain types of data or applications into the cloud. Topping the list includes things such as confidential financial data, credit card data, and sensitive IP. For firms especially concerned about security, possibly due to the industry vertical they operate in, the likelihood to withhold certain types of data or applications is even more pronounced.

INQUIRIES WHEN ASSESSING CLOUD PROVIDER SECURITY



Source : CompTIA's *9th Annual Information Security Trends* study Base: 340 U.S. Companies Using Cloud Computing

For IT solution providers and cloud service providers, this should serve as a reality check. Yes, the cloud is an important trend and will affect their business (see *CompTIA Channel Partner Trends* study for more details on this topic), but there will still be a need for robust on-premise solutions for many years to come.

TIP #4. KNOW COMPLIANCE REQUIREMENTS...YOUR OWN AND YOUR CUSTOMERS'

Recently, the City of Los Angeles and Google learned the hard way what happens when an uncertain regulatory variable is introduced into a cloud deployment. LA had to alter its plan to shift 30,000 city employees to Google Apps when it was discovered the software was not fully compliant with the FBI's security requirements for connecting to the Criminal Justice Information System (CJIS), a clearinghouse of law enforcement data administered by the Department of Justice.

This is one notable example of what is sure to be a more regular occurrence – organizations making the transition to the cloud only to discover a security related element that forces a change of plans. As the cloud model matures, some of these issues may naturally work themselves out, but in the shorter-term, IT solution providers and cloud vendors can provide a valuable service in reducing the likelihood of these types of situations. Longer term, third party assessments of cloud service provider security policies, procedures, and capabilities may become standard. (See the *CompTIA Quick Start Guide to Security Compliance* for additional information and resources on compliance requirements for different industries.)

TIP #5: APPRECIATE THAT LINE OF BUSINESS MANAGERS OFTEN VIEW SECURITY DIFFERENTLY...IF AT ALL

One of the most discussed aspects of cloud computing is its accessibility, even for users who have lower amounts of technical skill. Spinning up a virtual machine in an IaaS environment does not require detailed knowledge of the hypervisor. An end user can start working with a SaaS application by visiting a website and providing user credentials and billing information. Cloud computing lowers the barrier of entry to technology and gives access to areas that have traditionally required cooperation with the IT department.

For this reason, the concept of "rogue IT" is gaining traction. This refers to the tendency of lines of business to use their own budgets

to procure resources. In conjunction with the consumerization of IT (where consumer trends, techniques, and technology are being used for business purposes), rogue IT presents a new challenge for the IT department. Certainly the concept is not unique to the cloud—in searching for the quickest way to a solution, end users have frequently used their own budgets to buy software or devices. The difference with cloud resources is that they are much more powerful and usable. The virtual machine in an IaaS environment may not require hypervisor knowledge, but it also does not require the actual purchase of a physical server, something that would not have fit into a standard line of business budget.

This represents a high-risk area for companies. Although cloud solutions remove the need for certain technical skills, part of the value in the IT department or the IT Service Provider is the knowledge of how technology fits into the overall business process and how to maintain a secure position. Business staff who begin using cloud solutions outside the purview of those responsible for the IT environment may not be considering where data is being stored, what happens in case of an outage, or how the cloud tool is integrated into other business systems. With security already a major concern for companies, this is another area to be aware of so that data remains confidential and compliance to required standards is maintained. It is also important to remember that the burden does not rest solely on the lines of business; IT departments also need to examine their policies and perceptions to ensure that they are not overemphasizing their preferences at the expense of business outcomes.

Even with High Confidence in Cloud Security, Many Firms Still Unwilling to Store Certain Types of Data There

Data companies are NOT yet willing to put in the cloud	SMALL FIRMS	MEDIUM FIRMS	LARGE FIRMS	SECURITY RATED A HIGH PRIORITY	SECURITY RATED A MEDIUM OR LOW PRIORITY
Confidential company financial data	49%	55%	56%	58%	42%
Credit card data	50%	50%	53%	56%	37%
Employee HR files	45%	43%	44%	43%	47%
Confidential intellectual property / company trade secrets	41%	42%	44%	48%	30%
Customer contact information	30%	35%	25%	30%	28%
Data covered by regulations (e.g. HIPPA, PCI, Sarbanes-Oxley, etc.)	25%	26%	25%	26%	24%

Source : CompTIA's *9th Annual Information Security Trends* study Base: 500 U.S. Companies

Cloud Security Guidance

The Cloud Security Alliance organizes guidance for addressing areas of concern with cloud computing into 12 domains, which are detailed in Security Guidance for Critical Areas of Focus in Cloud Computing v. 3.0. The full publication can be found here:

https://cloudsecurityalliance.org/research/security-guidance/.

The 12 domains are grouped into two categories: governance and operations. The governance domains are broad and address strategic and policy issues within a cloud computing environment, while the operational domains focus on more tactical concerns and implementation within the architecture.

GOVERNANCE DOMAINS

- **Governance and Enterprise Risk Management**
  The ability of an organization to govern and measure enterprise risk introduced by cloud computing. Legal precedence for agreement breaches, ability of user organizations to adequately assess risk of a cloud provider, responsibility to protect sensitive data when both user and provider may be at fault, and the affect of international boundaries are some of the items discussed.
- **Legal Issues: Contracts and Electronic Discovery**
  Potential legal issues when using cloud computing. Issues addressed include protection requirements for information and computer systems, security breach disclosure laws, regulatory requirements, privacy requirements, international laws, etc.
- **Compliance and Audit**
  Maintaining and proving compliance when using cloud computing. Issues dealing with evaluating how cloud computing affects compliance with internal security policies, as well as various compliance requirements (regulatory, legislative, and otherwise) are discussed here.
- **Information Lifecycle Management**
  Managing data that is placed in the cloud. Items surrounding the identification and control of data in the cloud, as well as compensating controls that can be used to deal with the loss of physical control when moving data to the cloud, are discussed here.
- **Portability and Interoperability**
  The ability to move data/services from one provider to another, or bring it entirely back in-house. Issues surrounding interoperability between providers are also discussed.

OPERATIONAL DOMAINS

- **Traditional Security, Business Continuity and Disaster Recovery**
  How cloud computing affects the operational processes and procedures currently used to implement security, business continuity, and disaster recovery. This section focuses on examining the possible risks of cloud computing, and calls better enterprise risk management models. Further, the section touches on helping people to identify where cloud computing may assist in diminishing certain security risks, or entails increases in other areas.

- **Data Center Operations**
  How to evaluate a provider's data center architecture and operations. This is primarily focused on helping users identify common data center characteristics that could be detrimental to on-going services, as well as characteristics that are fundamental to long-term stability.
- **Incident Response, Notification and Remediation**
  Proper and adequate incident detection, response, notification, and remediation. This attempts to address items that should be in place at both provider and user levels to enable proper incident handling and forensics. This domain will help you understand the complexities the cloud brings to your current incident handling program.
- **Application Security**
  Securing application software that is running on or being developed in the cloud. This includes items such as whether it's appropriate to migrate or design an application to run in the cloud, and if so, what type of cloud platform is most appropriate (SaaS, PaaS, or IaaS).
- **Encryption and Key Management**
  Identifying proper encryption usage and scalable key management. This section is not prescriptive, but is more informational in discussing why they are needed and identifying issues that arise in use, both for protecting access to resources as well as for protecting data.
- **Identity and Access Management**
  Managing identities and leveraging directory services to provide access control. The focus is on issues encountered when extending an organization's identity into the cloud. This section provides insight into assessing an organization's readiness to conduct cloud-based Identity, Entitlement, and Access Management (IdEA).
- **Virtualization**
  The use of virtualization technology in cloud computing. The domain addresses items such as risks associated with multi-tenancy, VM isolation, VM co-residence, hypervisor vulnerabilities, etc. This domain focuses on the security issues surrounding system/hardware virtualization, rather than a more general survey of all forms of virtualization.

A good resource for the types of security questions that should be considered when evaluating cloud service providers comes from the Cloud Security Alliance (CSA). This not-for-profit organization provides a useful list of over 200 questions covering data integrity, security architecture, audits, regulatory compliance, governance, physical security, legal and more. The document can be accessed here: https://cloudsecurityalliance.org/research/cai/

CompTIA

Powered by

CompTIA.org