Jefferson Wells™
ManpowerGroup

Emerging Insight…

Cloud Security & Governance

Cloud computing is quickly becoming the rule vs. the exception. Over half of all systems and data are now stored in the cloud. There are many advantages to leveraging cloud computing, but just as many risks too. Organizations depend on cloud computing for managing and storing customer data, financial accounting and reporting, and fulfillment of core business processes. Managing the cyber aspects of cloud computing is a critical concern.

Threat and Mitigation Strategies for Cloud Computing

Abuse and Malicious Use of Cloud Computing

- Stricter initial registration and validation processes
- Enhanced credit card fraud monitoring and coordination
- Comprehensive monitoring of customer network traffic
- Monitoring public blacklists for one's own network IP blocks

Insecure Interfaces and APIs

- Analyze the security model of cloud provider interfaces
- Ensure strong authentication and access controls are implemented in concert with encrypted transmission
- Understand dependency chain associated with API interfaces

Unknown Risk Profile

- Disclosure of applicable logs and data
- Ascertain details of provider's infrastructure
- Monitoring and alerting triggers

Malicious Insiders

- Implement role-based access controls and multifactor authentication
- Specify background checks as part of the hiring process
- Require transparency into overall information security and management practices, as well as compliance reporting
- Determine security breach notification processes

Shared Technology Issues

- Enforce strict supply chain management and conduct a comprehensive vendor assessment
- Implement security best practices for installation and configuration
- Monitor environment for unauthorized changes and activity
- Promote strong authentication and access control for privileged access
- Enforce service level agreements for patching and vulnerability remediation
- Conduct vulnerability scanning and configuration audits

Characteristics

- On demand service
- Broad network access
- Resource pooling
- Rapid elasticity
- Measured service

Service Models

- SaaS
- PaaS
- IaaS

Deployment Models

- Private
- Community
- Public

Data Loss or Leakage

- Implement strong API access control
- Encrypt and protect integrity of data in transit
- Use DLP solutions for endpoint devices and gateways
- Analyze data protection in both Development and Production
- Implement strong key generation, key storage and management, and key destruction practices
- Contractually require providers wipe persistent media before it is released into the pool for reuse
- Contractually specify provider backup and retention

Account or Service Hijacking

- Implement RBAC to limit damage in case of compromise
- Prohibit sharing of users and services account credentials
- Leverage strong multifactor authentication techniques
- Use proactive monitoring to detect unauthorized activity
- Fully understand cloud provider security policies and SLAs

Case Study: Conducting an Assessment of Cloud Security & Governance

Discovery

Copies of policies, procedures and supporting information was requested from management. As documentation was reviewed, it quickly became evident that any governance over cloud computing was occurring primarily at the individual business unit level as opposed to taking place with IT.

Because of this, in addition to the core IT group that supported cloud computing, a significant amount of review effort focused on interviewing leadership and key stakeholders within the business units to understand the current control environment rather than relying solely on the documentation to determine potential risk mitigation issues and identify policy and procedural gaps. In addition to the core IT group who support cloud computing, the interviews during discovery and analysis tasks included key stakeholders from multiple business units within the organization.

Analysis

The key activity in this phase is to identify any critical business or program risks, controls gaps and improvement opportunities discovered during documentation reviews and interviews. Working with a client liaison throughout the analysis phase, additional stakeholder interviews were needed to gather additional information. The focus of these interviews was to better understand the controls and processes used in management, operations and support areas that would involve the collection, storage, or processing of various forms of sensitive information in the cloud computing environment. After the gaps were identified, recommendations for corrective actions were developed to address each observation.

Reporting

Using the information acquired and analysis results, an executive summary report is developed to outline the assessment of the organization’s current cloud computing governance, and recommended actions to address the gaps and identified opportunities. The primary goal of the report is to provide a set of pragmatic recommendations enabling the organization to better understand inherent and latent cloud governance risks and have greater confidence the deployed controls and processes would enable them to meet the information privacy mandates and control obligations imposed by legal, regulatory, contractual and industry requirements.

The observations and recommended actions identified during the review were categorized into four major risk areas: Cloud Governance, Information Protection, Vendor Management and Regulatory Risk.

Findings

Cloud Governance

No centralized oversight or tracking to monitor which cloud vendors are utilized, what types of data are stored in the cloud, or how this data is being protected and backed up. This sets up a scenario where management may be incurring significant risk without the knowledge of senior management.

Specifically:

- No policies or other guidance documents currently released in the policy portfolio establishing data classification, or marking and handling requirements that must be implemented to properly designate sensitive and business critical information
- No centralized register identifying cloud applications and providers, or whether ePHI was stored
- Cloud-based applications did not appear to be adequately addressed in business continuity planning

Information Protection

The practice of decentralized governance over cloud-based applications has led to departures from organizational security practices which places data at risk.

Specifically:

- No automated access controls under the control of agency management requiring the use of strong passwords in cloud-based applications
- No assurance that ePHI and other sensitive data stored in the cloud is always encrypted
- Cloud-based applications were not subject to a security vetting process prior to implementation

Vendor Management

There were significant inherent security risks noted that needed to be addressed through implementing formal vendor security control requirements and vendor risk reviews. Contractual requirements for periodic risk assessment, and mandatory logging, monitoring, and reporting were lacking in order to reduce the firm's risk exposure and potential legal liability if one of these vendors is breached.

Specifically:

- No formal vendor management vetting process for selection and retention of cloud vendors
- No contractually binding requirements in place requiring vendor adherence to the organization's vendor data privacy requirements
- Cloud vendors had not provided SOC2 Type II reports

Regulatory Risk

As there was no centralized oversight of cloud-based computing, sensitive information was not classified and marked, and cloud vendors were found to be loosely controlled and monitored. It is difficult for personnel to determine to what extent the organization may be out of compliance with federal, state, and local laws and regulations.

Specifically:

- No mechanism or process for identifying and recording the types of data stored in the cloud, including health data subject to regulations
- No formal process for ensuring data stored in the cloud adheres to HIPAA or data privacy regulations

Authored by

Stephen Head
National Practice Leader, Cyber Risk Center of Expertise
704.953.6688
stephen.head@jeffersonwells.com

Stephen has broad-based experience in cyber risk, regulatory compliance, and IT governance. He is the author of the internationally recognized *Internal Auditing Manual* and *Practice IT Auditing*, both published by Thomson Reuters. He served as international chair of the ISACA Standards Board, served on the AICPA National Accreditation Commission, and on the AICPA Information Technology Executive Committee. Stephen is a CPA, CISSP, CISM, CDPSE, CMA, CFE, CISA, CGEIT, CRISC, CBCP, MCSE, CHP, CHSS, CITP, CGMA, CPCU, and holds an MBA from Wake Forest University.