Managing Cloud Risk

Top Considerations for Business Leaders

Do you have something to say about this article?
Visit the *Journal* pages of the ISACA web site *(www.isaca.org/journal)*,find the article and click on the Comments link to share your thoughts.

Phil Zongo
Is a cybersecurity consultant based in Sydney, Australia. He has more than 10 years of technology risk consulting and governance experience working with leading management consulting firms and large financial institutions. He recently led a successful risk assessment initiative for a complex, multimillion-dollar cloud transformation program.

Cloud adoption continues to grow at a rapid pace, transforming businesses across the globe. In fact, cloud is now business as usual for most organisations, with some utilising it to run business-critical processes. In July 2015, the ISACA® *Innovation Insights* report[1] cited cloud computing as one of the leading business trends driving business strategy. It ranked third out of 10 top emerging technologies most likely to deliver significant business value in excess of cost. Big data analytics and mobile technologies ranked first and second, respectively. A separate publication by International Data Corporation (IDC) forecasts worldwide use of public cloud growing at 19.4 percent annually over the next five years, nearly doubling from approximately US $70 billion in 2015 to more than US $141 billion in 2019. This is almost six times the growth of enterprise IT spending as a whole.[2]

Whilst cloud promises significant benefits, including enhanced financial flexibility, improved agility and access to leading technologies, some organisations are still holding back, mostly wary of losing control over high-value information. These risk concerns are valid and, if not properly considered and managed, may result in detrimental business impacts, including degraded customer experience, sensitive data breaches or brand damage.

This article provides some practical recommendations to address three key areas of risk associated with cloud adoption:

1. Cloud initiatives not aligned with business strategies
2. Loss of control over high-value information
3. Overreliance on cloud service providers

This is not a definitive or complete set of risk areas that businesses might face when adopting cloud computing. Several frameworks, most notably from the Cloud Security Alliance (CSA), ISACA®, and the US National Institute of Standards and Technology (NIST), provide more comprehensive guidance on managing cloud risk.

Aligning Cloud Projects With Business Strategy

Enterprises deliver shareholder value by taking on risk, but fail when the risk is not clearly understood and effectively managed. Often, cloud projects are IT-driven and technology-centric. To deliver business value and minimise risk exposure, such initiatives should be fully aligned to business strategies. Active engagement and oversight by the board or relevant risk governance committees are essential prerequisites for cloud program success.

In its June 2012 publication, *Enterprise Risk Management for Cloud Computing*,[3] the Committee of Sponsoring Organizations of the Treadway Commission (COSO) emphasised that the responsibility for cloud risk management starts right at the top. The paper stated, 'Cloud computing should be considered in the organization's overall governance activities and regarded as a topic warranting discussion and inquiry by an organization's board'. The board should determine what cloud services are appropriate to the business, based on enterprise goals, risk appetite and tolerance. But this is not always the case.

The Australian Prudential and Regulatory Authority (APRA), in a cloud information paper published in July 2015,[4] raised a concern that cloud reporting by regulated entities to boards of directors (BoDs) mostly focused on the benefits, while failing to provide adequate visibility of associated risk. Effective cloud risk management requires the board to challenge the adequacy of risk measures against appetite and business strategy. To enable this, pertinent information should be provided, including:

- Cloud value proposition, traceable links to business strategy and how benefits will be measured
- Top business risk and treatment strategies, i.e., data security, privacy laws, data location, business resilience, regulatory compliance
- Proposed cloud deployment model: public, private or hybrid and associated risk implications
- Planned cloud service delivery model: Software as a Service (SaaS), Platform as a Service (PaaS) or Infrastructure as a Service (IaaS), and associated risk implications
- Service provider selection criteria, including financial viability, operational stability and cybersecurity capabilities
- Plausible business disruption scenarios and recovery plans

- Service level agreements (SLAs), incident response and operational governance
- Third-party assurance, penetration testing, vulnerability assessments and right-to-audit clauses

Cloud initiatives should start with identifying business problems and strategic objectives and then build solutions to address business-specific needs. Clear, ongoing communication of cloud value and the risk management approach is critical to gaining business buy-in into cloud programs and achieving their ultimate success.

Protecting High-value Information

Managing cyberrisk without restricting business innovation and agility is a critical business imperative. Although cloud providers continue to invest heavily in security capabilities, concern about data security and regulatory compliance remains one of the key barriers to cloud adoption. In 2015, The Economist Intelligence Unit, in collaboration with IBM, conducted a global cloud maturity study. The results of this multiphased research, which reflected upon the perspectives of 784 stakeholders (including board members, chief executive officers [CEOs], chief financial officers [CFOs], chief information officers [CIOs] and other C-level executives) globally, revealed data security as the top likely negative influence to cloud adoption over the next three years, proving that some business executives are not yet convinced about cloud security. These concerns are further heightened by new risk presented by elements of the public cloud, in particular:[5]

- **Multitenancy**—Computing capacity, storage and network are shared across multiple cloud customers. Whilst this model allows cloud providers to achieve economies of scale and lower service costs, there is increased risk that a single vulnerability or misconfiguration can lead to a compromise across multiple customers.
- **Shared responsibilities**—Migrating business applications to the cloud creates a model of shared responsibilities between cloud customers and service providers. Customers relinquish some key responsibilities to the service provider, e.g., physical access and infrastructure management.

The European Union Agency for Network and Information Security (ENISA) asserts that massive concentrations of resources and data in the cloud present a more attractive target for cybercriminals.[6] Furthermore, cloud security breaches garner wider media coverage, which amplifies the impact of such incidents. Extensive media coverage of the 2014 Apple Cloud breach, which exposed pictures of celebrities, underscores this point.

There are three critical security controls to protect high-value information in the cloud: information classification, encryption and privileged access management.

Identify High-value Information Assets
Data classification is a vital step toward building an effective cloud security control environment. Information owners should be engaged to assess and classify information assets based on business risk. This eliminates unnecessary security expenditure, as more resources are invested to protect the 'crown jewels'.

Data criticality differs from one organisation to the next, depending on the industry sector or corporate objectives. Insurance companies, for example, may be concerned with the privacy of their customers' health information, whilst high-tech firms may be concerned about the security of their product development plans.

Information that would be of high value to cybercriminals should also be considered. In September 2014, a Reuters article stated that medical information is now worth 10 times more than credit card numbers on the black market and is increasingly being targeted by cybercriminals.[7] Other high-value information targeted by cybercriminals includes business plans, pricing models, partnership agreements, emails for business executives and personal financial records.

As illustrated by **figure 1**, classifying information enables business leaders to make informed decisions regarding how much risk they want to take in pursuit of innovation. For example, an organisation may have no appetite to host highly confidential information in public cloud systems, yet have the appetite to utilise public cloud systems to host public information.

Isolate High-value Information

Once data has been classified, regulated enterprises may consider using a private cloud to isolate high-value applications. Private clouds, where a business owns and manages its own virtual environment, offer an opportunity to realise the benefits of the cloud whilst eliminating multitenancy and shared responsibility concerns. Previously, some organisations avoided private clouds due to the high set-up costs. The Verizon *2016 State of the Market—Enterprise Cloud Report* revealed that the cost of a private cloud is decreasing, providing organisations with safer, cost-effective environments to host high-value systems.[8]

Encrypt Sensitive Data

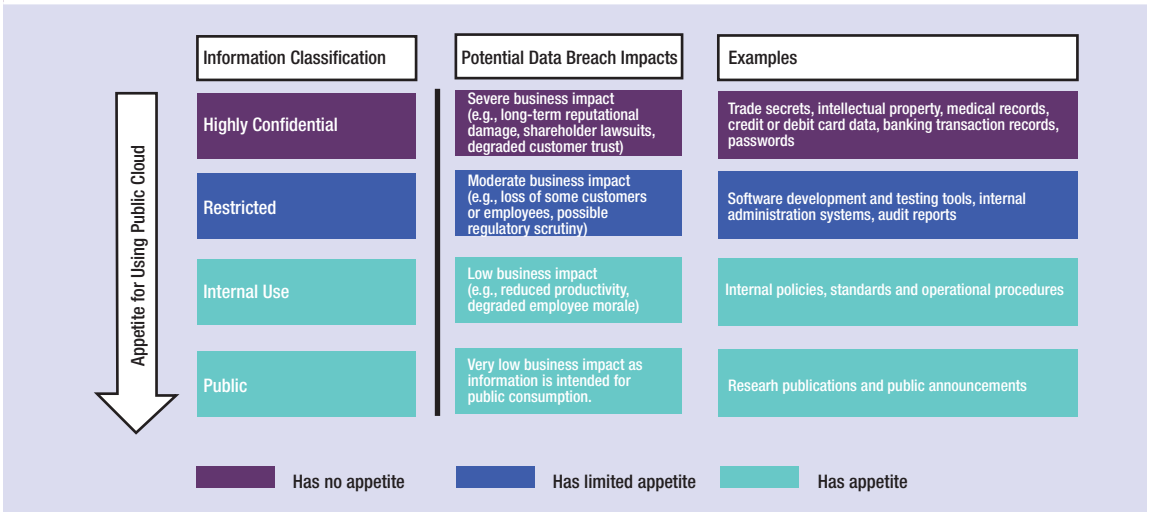
According to the CSA's September 2012 cloud encryption publication, *SecaaS Implementation Guidance, Category 8*,[9] encryption and protection of cryptographic keys are among the most effective data protection controls. High-value information should be encrypted when hosted in the cloud to minimise the risk of unauthorised disclosure. Robust key management is essential because losing encryption keys may result in data loss. The following recommendations should be considered when implementing encryption in the cloud:

- Implement tight controls to protect cryptographic keys, including a key life cycle management policy. NIST *Special Publication 800-57*[10] parts 1, 2 and 3 provide more detailed encryption key management guidelines.
- Ensure cloud encryption service includes disaster recovery and failover capabilities to minimise business impact if keys are lost.
- Define responsibilities for managing encryption keys. Retain key management to mitigate external breach of the service provider or malicious compromise by the service provider's privileged users.
- Test to confirm database encryption will not adversely impact application performance.
- Implement controls to purge data once removed from cloud storage.
- Complement data encryption with integrity protections such as digital signatures to maintain data authenticity.

Deploy Strong Controls Over High-privileged Access

Managing privileged access is critical to securing data in the cloud. Privileged accounts remain an ideal attack vector for cybercriminals because they

Figure 1—Information Classification for Cloud Adoption (Illustrative Example)



Source: Phil Zongo. Reprinted with permission.

provide unlimited access to high-value applications and data. A CSA February 2016 publication, *The Treacherous Twelve: Cloud Computing Top Threats in 2016*,[11] identified account hijacking, usually with stolen credentials, as one of the top cloud security threats. The dynamic nature of cloud computing amplifies existing privileged user risk in a number of ways, including:

- Certain cloud access roles are extremely high risk and have the potential to shut down entire cloud environments.
- The shared responsibilities model implies that cloud service administrators may have privileged access to an organisation's infrastructure, applications or databases, depending on the service delivery model. This increases the attack surface.
- The speedy and seamless provision of new virtual servers rapidly introduces new privileged accounts to an environment. These accounts are often created with default passwords, which are an easy target for cybercriminals to exploit.
- Cloud administrators can provision new virtual server instances at the click of a button. If relevant authorisation is bypassed, this may result in unplanned expenses, undermining an organisation's cloud business case.

The following people, processes and technology controls can help reduce this exposure:

- Confirm the effectiveness of a cloud service provider's privileged access controls specifically hiring and oversight of system administrators.
- Implement strong passwords and automate security policy provisioning.
- Enforce two-factor authentication and two-person rule over high-impact activities.
- Log and monitor access to privileged accounts, including execution of high-impact commands.
- Retain superuser account credentials for accounts that give full access to all cloud resources.
- Regularly rotate passwords for service accounts, using an automated password management solution.

A number of cloud service providers have specific guidelines on how these controls can be implemented within their environments. For instance, the Amazon Web Services (AWS) Security Blog[12] provides detailed guidance for managing privileged accounts within AWS.

Minimising Reliance on Cloud Service Providers

Improving service availability remains one of the key drivers for cloud adoption. Well-designed cloud solutions can significantly enhance business resilience as service providers continue to improve platform resiliency through clustering, replication and high-availability offerings.

In spite of these improvements, outages impacting multiple cloud service locations still occur. If not carefully planned for, these events may result in major supply chain and operational disruptions.

The good news is that reliable statistics are now available for businesses to assess cloud service reliability across different providers. For instance, Cloud Harmony, a third-party cloud vendor monitoring firm, provides independent comparison of cloud services based on service availability.

The following recommendations will help businesses mitigate these rare, but high-impact events:

- Review the cloud service provider's business continuity plan and disaster recovery plan to determine if they meet the organisation's recovery objectives.
- Utilise multiple cloud service providers to reduce risk of vendor lock-in.
- Implement high-availability cloud architecture to minimise service interruption.
- Complement the resilient architecture with regular backup and restore procedures, and store backup data outside of the cloud provider premises.
- Update and test the organisation's crisis management plan.

- Simulate recovery from different disaster scenarios, including recovery of individual applications, virtual environments and the entire cloud service provider.

From time to time, organisations terminate outsourcing arrangements—cloud arrangements are not an exception. Factors such as failure to meet performance requirements, security breaches or bankruptcy could lead to contract termination. To maintain business continuity and facilitate smooth transitions, organisations should formulate exit strategies or contingency plans to migrate critical records to an alternate solution, cloud or non-cloud.

Conclusion

When properly planned, implemented and governed, the cloud can be a major catalyst for process improvement as well as a driver of business transformation. Cloud service providers are working relentlessly to improve their security and resilience capabilities. In reality, an organisation's onsite systems may not be more secure than the cloud. Security and reliability risk may not outweigh the lost opportunity to transform an enterprise with strategic use of the cloud. Cloud initiatives built upon enterprise strategy, coupled with robust risk management processes, have the potential to accelerate business innovation, transform customer experiences and improve competitive advantage.

Acknowledgements

The author would like to thank Gina Francis, Innocent Ndoda, Kathleen Lo, Andrew Strong and Joe Chidwala for the valuable comments that helped improve this article.

Endnotes

1 ISACA, *Innovation Insights: Top Digital Trends That Affect Strategy*, USA, 2015, *www.isaca.org/Knowledge-Center/Research/Pages/isaca-innovation-insights.aspx*

2 IDC, "Worldwide Public Cloud Services Spending Forecast to Double by 2019, According to IDC," USA, 21 January 2016, *www.idc.com/getdoc.jsp?containerId=prUS40960516*

3 Chan, W.; E. Leung; H. Pili; *Enterprise Risk Management for Cloud Computing*, Committee of Sponsoring Organizations of the Treadway Commission, June 2012, *www.coso.org/documents/Cloud%20Computing%20Thought%20Paper.pdf*

4 Australian Prudential Regulation Authority, *Outsourcing Involving Shared Computing Services (Including Cloud)*, 6 July 2015, *www.apra.gov.au/AboutAPRA/Documents/Information-Paper-Outsourcing-Involving-Shared-Computing-Services.pdf*

5 The Economist Intelligence Unit, *Mapping the Cloud Maturity Curve*, IBM, 2015 *http://public.dhe.ibm.com/common/ssi/ecm/ku/en/kul12355usen/KUL12355USEN.PDF*

6 ENISA, *Cloud Computing—Benefits, Risks and Recommendations for Information Security,* Greece, December 2012, *https://resilience.enisa.europa.eu/cloud-security-and-resilience/publications/cloud-computing-benefits-risks-and-recommendations-for-information-security*

7 Humer, C.; J. Finkel; 'Your Medical Record Is Worth More to Hackers Than Your Credit Card', Reuters, 24 September 2014, *www.reuters.com/article/us-cybersecurity-hospitals-idUSKCN0HJ21I20140924*

8 Verizon, *State of the Market: Enterprise Cloud 2016*, 2016, *www.verizonenterprise.com/enterprise-cloud-report/*

9 Cloud Security Alliance, *SecaaS Implementation Guidance, Category 8: Encryption*, September 2012, *https://downloads.cloudsecurityalliance.org/initiatives/secaas/SecaaS_Cat_8_Encryption_Implementation_Guidance.pdf*

10 National Institute of Standards and Technology, *Special Publication 800-57*, USA, *http://csrc.nist.gov/publications/PubsSPs.html#SP 800*

11 Cloud Security Alliance, *The Treacherous Twelve—Cloud Computing Top Threats in 2016*, USA, 2016, *https://downloads.cloudsecurityalliance.org/assets/research/top-threats/Treacherous-12_Cloud-Computing_Top-Threats.pdf*

12 Amazon Web Services, AWS Official Blog, *http://aws.amazon.com/blogs/aws/*