Torkin Manes
Barristers & Solicitors

Article

Technology, Privacy & Data Management

July 2020

Safety first! New Canadian cloud security guidance is issued

Canadian Centre for Cyber Security releases guidelines for acquiring secure cloud services

By Lisa R. Lifshitz

In early June the Canadian Centre for Cyber Security (CCC) released four critical sets of guidelines for acquiring secure cloud services. While the CCC – Canada's federal cyber security organization operating under the Communications Security Establishment – originally created this advice and guidance for the Government of Canada, it will apply to any organization that wishes to move to a cloud-based environment.

Although organizations are attracted to the efficiency, scalability and elasticity of cloud services, security concerns remain, particularly for multitenancy public clouds that require sharing of computing, network and storage resources. The infrastructure failures or configuration errors of a cloud service provider (CSP) can negatively affect the confidentiality, integrity, and availability of an institution's data. Users of cloud services also have limited control and visibility on the cloud components that are exclusively the CSP's responsibility; as well, large cloud service providers present juicy targets to bad actors and remain vulnerable to intrusion and hackers.

Yet companies can also gain potential security benefits through cloud adoption. Most small- to medium-sized organizations don't have the resources to develop and maintain high security standards, and CSPs have clear incentives and resources to build experienced security teams and implement advanced security solutions to protect the cloud infrastructure and the services they provide. Most CSPs possess many security capabilities – including encryption, high availability groups, and multifactor authentication – and for additional fees may offer advanced threat detection, security and compliance monitoring, and reporting.

Cloud platforms also offer templates, automation tools, and scripting language that can be used to enforce and report on security baseline configurations, resulting in less effort to enforce compliance and fewer configuration errors. Many CSPs also seek and obtain third-party certifications, such as ISO/IEC

270018:2019, which ensure the third party will confirm that the CSP meets particular industry regulations and standards.

As well, large CSPs possess considerable resources and are more likely to withstand targeted intrusions, including distributed denial of service attacks. CSPs can distribute cloud workloads to multiple data centres around the world to guard against infrastructure failures and minimize the impact to customers during periods of cloud infrastructure maintenance.

Lastly, some CSPs offer storage, backup, and recovery capabilities that exceed those typically available to smaller enterprises, ensuring geo-redundancy of data and resilient backups. The backup and restore capabilities offered by CSPs may also allow companies to achieve a faster recovery of data following a technology failure.

The CCC's "Guidance on the Security Categorization of Cloud-Based Services" document focusses on determining an organization's security categorization in order to identify potential injuries that could result from security breaches. The Guidance is intended to help organizations categorize the security of cloud-based services and choose the security control profile that best protects an organization's information and business activities, and to act a guide when selecting a cloud deployment model and a cloud service model.

The Guidance recommends that before acquiring cloud based services, organizations should engage in the following security categorization activities: (i) develop an injury assessment table; (ii) create an inventory of business activities, processes, and information assets; and (iii) assess injuries resulting from business process and information asset failures.

Injury types may be determined by reviewing existing impact, privacy impact, business risk and threat and risk assessments. Entities may also develop injury types from business goals, objectives, and performance statements. Examples of injury types include (i) loss of reputation; (ii) loss of privacy (data under the organization's responsibility); (iii) regulatory fines (government regulations); (iv) contractual penalties (non-compliance with existing contracts); (v) harm to customer satisfaction; (vi) loss of intellectual property; (vii) loss of revenue/loss of business; (viii) loss of competitive edge; (ix) loss of shareholder confidence; and (x) increased legal cost.

The Guidance also suggests that creating an inventory of business processes and information assets is the most important step in identifying how organizations are affected by compromises to the cloud-based services. It will determine security controls for the organization and what high-level requirements are needed for an information system (and cloud system) to protect the confidentiality, integrity and availability of the organization's IT assets. The cloud security control profiles contained in the Guidance identify the recommended security controls that the CSPs and cloud consumers should jointly implement for the organization's various business functions. The selected cloud control profile also serves as the basis for assessment of the security controls.

When considering moving to the cloud, organizations often fail in one critical area: determining their appropriate cloud deployment model and cloud service model for IT services. It may sound obvious, but not all cloud services are the same. The National Institute of Standards and Technology has identified four cloud deployment models – public, private, community and hybrid – and three commonly used cloud services models: Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS), although other cloud service models exist (e.g., storage as a service, managed platform as a service). The Guidance advises that a customer's selection of a cloud deployment model and a service model should depend on the nature of the services it requires, the amount of control it wants to retain, and the level of expertise and maturity the customer has in operating and maintaining cloud based information systems. However, the information collected by the organization during the course of the security analysis described above should also be used to help select the cloud deployment model and the cloud service model that best matches the customer's internal expertise and required security assurance levels.

If security is a critical concern, prospective cloud customers should consider cloud models that have been assessed to meet the required security category requirements, selecting a deployment model and service model that require the least amount of additional effort to address and compensate for a CSP's security shortcomings. Considerations include: (i) an organization's information system strategies; (ii) the CSP's

cloud services capabilities and security control gaps; (iii) the security category of the business process to be supported by the cloud service; and (iv) selected security control profile requirements.

The cloud deployment models all offer various advantages and disadvantages. For example, the most common cloud model – public cloud – will offer standardized cloud services, some security protection and (usually) service level agreements. If an entity has very strict security, operational, or governance requirements, then an organization may need to implement compensatory controls to address gaps in the CSP's offerings, or consider other deployment models (e.g., private clouds). And because the public cloud model offers a multitenant environment, an organization will not normally be able to audit the security of the CSP environment and must rely on third-party assessments.

In the private (on-premises) cloud deployment model, the cloud infrastructure is provisioned for exclusive use by a single organization. It may be owned, managed, and operated by the organization, a third party, or some combination of them, and it may exist on or off premises. While typically more expensive, customers will find greater flexibility in negotiating services, operational processes, service level agreements, security, and governance requirements.

Another option, the hybrid cloud, is a combination of on-premises IT infrastructure with one or more of public, private or community cloud. Managing a hybrid cloud model comes with added complexity, because organizations must perform a security assessment of multiple CSPs, determine which security features to use from each cloud, manage resources from different CSPs, and determine location of resources and how to interconnect the different cloud environments securely.

Prospective cloud consumers should also consider their security requirements when choosing a cloud service model. SaaS users mainly use the provider's applications, whereas PaaS provides the consumer with the capability to deploy their own consumer-created or acquired applications created using programming, libraries, services, and tools supported by the provider onto the cloud infrastructure. IaaS provides the consumer with the capability to provision processing, storage, networks, and other computing resources with which to deploy and run various software, including operating systems and applications. The IaaS model allows consumers to tailor, implement and manage their own security controls, whereas the PaaS and SaaS models have much less flexibility.

The second Guidance document, "Guidance on Defence in Depth for Cloud-Based Services," is a much more technical document focussing on defence in depth and the layered approach when implementing security controls, and how this approach is used to protect against the risks associated with cloud computing.

The third Guidance document, "Guidance on Cloud Security Assessment and Authorization," stresses the reality of the shared service model; organizations have certain obligations for securing different components of the infrastructure and systems and cannot simply offload all responsibility to the cloud provider (tempting as that is).

Finally, the fourth document, "Guidance on cloud service cryptography," describes the role cryptography plays in protecting customer information and privacy when moving to a cloud-based computing model.

While it is unlikely that users of cloud services will ever find their security concerns to be completely mitigated, collectively the CCC's Cloud Guidance security documents offer useful information regarding the importance of security considerations in choosing and adopting the right cloud service. The Guidance also serves as a reminder that by understanding and implementing the appropriate layers of security for each organization, cloud computing can be implemented by companies with a reasonable degree of safety.

This article originally appeared in Canadian Lawyer.

Author

Lisa R. Lifshitz
Partner

Tel: 416 775 8821
llifshitz@torkinmanes.com

Lisa R. Lifshitz is a partner in Torkin Manes' Business Law Group, specializing in technology and privacy law, and is the leader of the firm's Technology, Privacy and Data Management Group. She has been nationally and internationally recognized for her technology law expertise and enjoys writing and speaking on technology law issues. She is the immediate past president of the Canadian IT Law Association.