Advisory for Web Buckets

The Office of the Information and Privacy Commissioner (OIPC) has seen an increase in reported breaches involving cloud storage containers, or "web buckets", that are unintentionally exposed publicly online, typically through misconfigured properties or settings.[1]

While most web bucket incidents reported to the OIPC are from private sector organizations, due to breach reporting requirements under the *Personal Information Protection Act* (PIPA), this advisory is for any organization that is using or considering the use of web buckets for the storage of personal or health information, such as public bodies or health custodians regulated by Alberta's *Freedom of Information and Protection of Privacy Act* (FOIP Act) or *Health Information Act* (HIA).

What Are Web Buckets?

Organizations are increasingly using external service providers to store data, run applications or otherwise deliver computing services "in the cloud".

Web buckets are one type of cloud service. Web buckets can be thought of as internet accessible containers, or folders, that store "objects" for various purposes, such as processing or to be displayed as content on websites. Objects are unstructured data or files (e.g. images, videos, documents, binaries, code, etc.)

How Web Buckets Are Exposed

Since data stored within web buckets is, by the nature of cloud computing, accessible via the internet, part of configuring buckets involves defining access permissions or controls, including setting who can read or write content for a bucket.

The contents of buckets are "exposed" when access permissions are misconfigured. For example, by mistakenly allowing unrestricted public access or providing access to all employees within an organization.

Misconfiguration of the buckets may result in unauthorized access and disclosure of an organization's data, which may include individuals' personal or health information.

Privacy and Security Considerations

Alberta's privacy laws require that reasonable steps be taken to protect against risks to personal or health information, which generally extends to service providers that host data on behalf of organizations.

Prior to using web buckets to store and process identifying information, organizations should conduct privacy and security risk assessments to identify, prioritize, and address risks that may affect the information.

[1] A breach means a loss of, unauthorized access to, or unauthorized disclosure of personal or individually identifying health information.

Office of the Information and Privacy Commissioner of Alberta

October 2020

Organizations should implement reasonable administrative, technical and physical controls to manage or address identified risks, including:

- **Complete a Privacy Impact Assessment (PIA)**

  A PIA is a process used for identifying and managing privacy and security risks associated with the collection, use, disclosure and retention of identifying information.

  PIAs should be conducted prior to implementing and operating web buckets.

  More information on how and when to complete a privacy impact assessment is available at **www.oipc.ab.ca**. Health custodians under Alberta's HIA are required to complete a PIA and submit it to the OIPC for review for any new or changed information system or administrative practice that involves the collection, use or disclosure of individually identifying health information.

- **Contracts and Agreements**

  Ensure that a signed contract is in place between your organization and the web bucket service provider that addresses:

  - Accountability and data ownership (i.e. who is responsible for personal information protection).
  - Data residency requirements (e.g. applicable legislation may require that personal information be stored within specific geographic locations).
  - How security incidents and privacy breaches will be managed, including steps that will be taken by the provider to ensure your organization is notified about the event in a timely manner.
  - How personal information will be securely returned to your organization and how copies in the provider's systems will be securely deleted upon termination of services.
  - Who may access personal or health information stored in the provider's systems, and the legal authority for such access (e.g. law enforcement).

  In addition to the above, ensure that your web bucket provider has reasonable privacy and security policies in place that govern its information handling practices.

  Understand what your cloud service provider is permitted to do with your records.

- **Encryption of Information**

  Ensure that information in buckets is encrypted at rest, and in transit, using industry standard cryptographic algorithms at minimum.

  Ensure your cloud provider implements reasonable administrative and technical controls for the security of encryption keys, if the provider manages encryption on behalf of your organization.

- **Logical Separation of Web Buckets**

  Ensure your cloud provider implements reasonable technical controls that logically separate your organization's personal information from that of other clients.

- **Web Bucket Access Controls**

  Ensure web buckets have reasonable access controls that are configurable, and align with your organization's privacy and security policies and practices. This includes having processes and policies in place that govern who approves and provisions access, and for terminating access to the buckets in a timely manner.

  Also ensure access permissions for buckets and their contents (objects) are configured in accordance with your organization's privacy and security policies so that authorized individuals access the least amount of information required to complete a task.

  Conduct periodic reviews of your access control settings to reasonably protect the information in the buckets and to ensure accounts that no longer need access to the buckets are removed.

  If your website accesses data from buckets, ensure visitors are only able to access the information required for the services that your organization provides. For example, for a bucket that requires public access, such as website

content, ensure that identifying information is not stored within the same public bucket as it may list its files and directories to any user.

- **Prepare for Incidents and Breaches**

  Implement an incident response plan, including processes and procedures for managing security incidents and privacy breaches.

  Understand your organization's role, and that of the service provider, in managing incidents and breaches.

  Perform periodic audits of accesses to information in your web buckets.

  Ensure information in the buckets is securely backed up and stored in an alternate location.

  Periodically test your backups for recoverability.

  Provide appropriate training to your staff.

Other guidance may prove helpful in identifying and addressing risks and understanding legal obligations to protect personal or health information. Resources, such as "Securing Personal Information: A Self-Assessment Tool for Organizations" and "Cloud Computing for Small- and Medium-Sized Enterprises", are available at **www.oipc.ab.ca**..

When a Breach Occurs

Despite policies and guidance, breaches still occur. If an incident occurs, the OIPC has guidance available entitled "Key Steps in Responding to Privacy Breaches" available at **www.oipc.ab.ca**.

Certain incidents under PIPA and HIA must be reported to the OIPC, and may voluntarily be reported under the FOIP Act.

The OIPC has guidance on its "How to Report a Privacy Breach" webpage at **www.oipc.ab.ca** for reporting breaches to the Information and Privacy Commissioner.

The OIPC may be able to provide general advice or guidance for responding to the privacy breach and ensuring steps are taken to comply with obligations under privacy legislation.