eSCRIBE

Keeping Public Sector Documents Safe in the Cloud

WHITE PAPER

As modern business systems increasingly shift from installable, on-premises software to subscription-based software-as-a-service (Saas), public sector organizations often find themselves wondering whether their documents are secure from theft, loss and destruction if they're stored in the Cloud. This paper will explore common cloud-related concerns of municipalities and other public entities, and compare the benefits and risks of cloud-based storage with those of storing data locally.

The use of cloud-based services and storage has become pervasive in today's society – from online banking and shopping to photo sharing and even filing your income taxes. However, many public sector organizations that have long hosted their documents internally on their own servers are still asking: "how secure are our documents if we store them in the Cloud?"

You may have your own questions about cloud data security, your council members may have concerns, or you may have encountered resistance to cloud services from an IT department wishing to maintain long-rooted processes. Concerns about cloud services often stem from people's inexperience with them; the Cloud is a relatively new paradigm, and a lack of familiarity can breed fear. The sections below will give you important background information you need to make informed decisions about the Cloud, providing an in-depth look at some common concerns of municipalities and other public entities while comparing the benefits and risks of cloud-based storage with those of continuing to store your data yourself.

The Bank vs. The Mattress

For individuals and organizations reluctant to move their data into the Cloud, most concerns revolve around the same fundamental concept: "my data is no longer in my control." While that statement may be largely true, there are measures you can take – not just from a technical perspective, but also from a contractual perspective with your cloud vendor – to minimize any negative impact of that shift. More importantly, though, your data is likely safer from modern threats in the hands of dedicated, third-party experts than it is with your own comparatively limited resources.

Would you store large sums of money under your mattress in your house, or would you trust it to a bank? Most rational people would put it into an accredited financial institution, knowing that the bank could secure it better than they ever could themselves. Similarly, reputable and proven vendors of cloud services offer levels of protection far beyond what most organizations could implement internally.

There are two core facets of keeping your data secure – security against theft, and security against loss or destruction. In the mattress vs. bank analogy, your house is at a higher risk of theft than the bank, as your residence is less difficult to break into physically. Banks also have sophisticated fire suppression systems and the like, putting them and their contents at lower risk of destruction than your mattress.

Overall, the bank has extensive security infrastructure, safety protocols, insurance and access authentication processes that would be prohibitively difficult and expensive for you to implement on your own. Cloud service providers offer the digital equivalent of these measures to secure your data, including:

- **Encryption.** For data to be secure it needs to be encrypted, which transforms the original information into a coded form intended only to be readable by authorized users with the right "key" to decode it. Encrypting your data while in transit between your computer and your storage repository keeps it from being stolen by anyone who intercepts the transmission. Protocols such as SSL (Secure Sockets Layer) protect data in transit; you can see SSL in action for yourself when transferring data through a web browser if the address is prefaced with HTTPS instead of HTTP. Meanwhile, having your data encrypted "at rest" (i.e. when already stored) prevents it from being usable by unauthorized parties if the storage is breached. Your organization or your cloud vendor may have corporate standards for the encryption protocols, methods and algorithms used for stored information. In both cases, encryption keeps your data secure: while it is moving to and from cloud-based storage, and once it arrives there.

- **Physical Security.** As always, whenever you try to protect your property – whether data or tangible goods – from theft or unauthorized access, your security is only as good as its weakest link. Whether you have laptops in the field that may become lost, computers sitting under desks, or even your own data centre locked with a passcode, your physical defenses are almost certainly less robust than the security measures cloud providers have surrounding their data centres. Cloud vendors' security is integral to their business, so they ensure that it is stronger than you could or would build yourself – from 24/7 security guards to reinforced structures and restricted access with biometric scanners. Just as a bank is far more physically secure than your mattress, cloud storage vendors' physical protection likely far exceeds your own.

- **Cybersecurity.** Encrypting data to prevent theft of information is just one element of cybersecurity; many of today's digital threats are designed simply to disrupt or extort money from businesses or governments by destroying data or preventing legitimate access to it. Ransomware, denial-of-service attacks and other threats are constantly evolving, and often leverage social engineering or outdated security patches to penetrate deeply within organizations' on-premises systems. With dedicated, full-time teams of cybersecurity experts, cloud vendors will almost certainly be more up-to-date on the latest threats and able to react more quickly to even "zero-day" attacks than your own in-house IT resources could.

- **Backups and Redundancy.** While almost every organization understands the need to back up their data, the majority of people don't sufficiently test the backups they make to verify that they can be properly restored. There's no worse time to find out your backups are unrecoverable than when you need them the most. Furthermore, if you create your own backups, it's your responsibility to store them across multiple locations; storing them at a single site leaves you vulnerable to a catastrophic event at that facility. With cloud services, your data can be automatically backed up redundantly across multiple physical locations – for example, it could be hosted in Quebec City with a backup or failover site in Toronto. In addition to safeguarding your information, mirroring it to a second site enables high-availability failover for quick and continued access even if the primary site suffers an extended outage. Going back to the bank analogy, if your closest bank branch suffered a fire, you can still go to another branch to get your money out. But if your house burned down, everything under your mattress would be gone forever.

Common Concerns

Even with all of these advantages, public sector organizations may still have apprehensions about cloud storage. Some of them aren't in fact directly security-related per se, and many such concerns can be alleviated contractually rather than technically.

- **Data Ownership.** A corollary to the "my data is no longer in my control" concern is the perception that "my data is no longer mine" once it's in the cloud. This is a legal consideration rather than a technical consideration, and there are things you can do as a customer to ensure that you retain ownership of your data. When negotiating contract terms with your cloud services vendor, make sure that the contract states unequivocally that the data is yours and yours alone. Also be sure that it documents that at the end of the contract your raw data will be returned to you in its original format, rather than in some converted or proprietary form. The contract must also specify that upon your authorized approval, the cloud vendor will destroy all copies of your data in their storage, with a certificate of destruction provided as a legally-binding guarantee.

- **Privacy.** Every jurisdiction, as well as particular public sectors, has one or more privacy standards that can vary significantly between them. In Ontario alone, for example, privacy legislation spans the Freedom of Information and Protection of Privacy Act (FIPPA), the healthcare-specific Personal Health Information Protection Act (PHIPA), Canada's federal Personal Information Protection and Electronic Documents Act (PIPEDA) and more – all of which may differ from their counterparts in other provinces or countries. Make sure that your vendor is aware of your jurisdiction's privacy standards, and their processes and contracts are compliant with them. To further protect yourself legally, make it a contractual requirement of your vendor that private data is truly kept private, with nobody able to access it – even within the vendor's own staff – without appropriate security clearance.

- **Lost Internet Connectivity.** It's true that if your facility loses its Internet connectivity, you'll temporarily lose access to your cloud-stored data during that outage. Fortunately, Internet connectivity is a lot more stable and high-availability than it used to be, and while it hasn't yet reached the "five-nines" reliability (99.999% uptime, averaging just 5.26 minutes of downtime per year) expected of mission-critical internal systems, it's starting to approach it. Any outages tend to be mercifully short, and technologies like SD-WAN can provide fault tolerance for your connectivity. More importantly in the big picture, if you lose Internet connectivity, access to your meeting management documents may be the least of your concerns. If your technology platforms are current, your software applications (such as Office 365) probably run on the Cloud too, or even your office phone routing system. Getting those services operational again will almost certainly be a higher priority for you than document access.

- **Cloud Vendor Demise.** As with any critical service that your organization depends on, it's important to choose your cloud vendor wisely; if your cloud storage host was to go out of business, your data could disappear with them in spite of what your contract states. The more risk-averse you are, the more you'll want your data held by one of the bigger cloud players. Amazon Web Services, Google and particularly Microsoft have all been around for a very long time, and their immense corporate size minimizes the likelihood of them folding. Choosing a large cloud vendor has other benefits too, as they conduct regular security audits and offer comprehensive disaster recovery plans, faster failover response times, and more robust SLAs. That doesn't mean your software application vendor itself needs to be a big company; many smaller innovators partner with the largest cloud platform providers to ensure their customers' data is secure. eSCRIBE, for example, runs on the proven Microsoft Azure platform.

Overcoming Apprehension

There's no question that the move of applications and storage to the cloud is a new paradigm for users to become comfortable with. As with any significant technological shift, the apprehension towards cloud storage tends to stem from unfamiliarity: "I don't understand it yet, so it must be a risk." In such cases, educating yourself and others in your organization will be critical in making informed decisions.

IT staff may also be concerned that cloud-based services take away some of the infrastructure responsibility that they're accustomed to, and that they may be held accountable for things that the Cloud moves out of their control. Involving the IT group in your discussions with cloud vendors can help alleviate those concerns, making sure all of their requirements are met and that all corporate security standards are addressed while reassuring IT staff that they still have a key role even in a more cloud-centric approach.

Ultimately, there are always security risks whether you store your data in the Cloud or on-premises, but the fundamental question is this: can cloud service providers implement better security than you could do yourself? The answer is almost always yes, as it's difficult, expensive and resource-intensive for organizations just to approach the security of the Cloud, let alone match it. Going back to our original analogy, by the time you've made your house and mattress equivalently secure to what a bank can offer, you've practically built your own bank branch – and you still don't have the dedicated resources or multiple locations to match the bank's full security capabilities.

Ask the Right Questions

With the above in mind, you'll be well-equipped for discussions with your prospective cloud vendors to ensure that they can meet your security requirements. As a brief recap, here are some of the key questions you should ask of the vendors you're considering:

- What information security standards is the cloud vendor compliant with?
- Is data encrypted both during transmission and at rest? And are the encryption protocols aligned with your corporate standards?
- Are the provider's processes and contract terms fully compliant with your specific jurisdiction's privacy standards?
- Does the contract state unequivocally that your data is yours, and yours alone? And what processes and policies do they have in place to enforce that?
- What options does the provider offer for multi-site backup and failover?
- What disaster recovery plans does the provider have in place?
- What are the contractually-guaranteed response times if an issue arises?
- Does the contract specify that your data will be returned to you in its original form at the end of your contract?

- Does the contact specify that all copies of your data will be verifiably destroyed upon your authorized instruction?

Satisfactory answers to these questions will go a long way to making yourself, your council members and your IT department comfortable with the safety and security of your data in the Cloud.

Embracing the Change

Even if you aren't yet convinced that you want to move your applications and documents to the Cloud, before long you may not have a choice. Many software vendors are moving towards exclusively offering their solutions as subscription-based cloud services; even Microsoft will discontinue sales of perpetual Office standalone software in favor of the subscription-based Office 365 in the not-so-distant future. Much like home phones have largely – but not completely – faded away in favor of cell phones, on-premises software solutions are doing the same.

As such, a move to the Cloud seems inevitable in your future. Embrace it, and you can reap the full advantages the Cloud offers. And you don't need to worry about whether your cloud-stored documents will be secure – with the right choices and careful attention to your cloud contracts, they'll even better-protected than they would be on-premises, making your own storage seem as quaint as the proverbial money-stuffed mattress.