GOING UP? SAFETY FIRST, THEN SEND YOUR DATA TO THE CLOUD

Joe Sturonis, CTO van PKWARE, schrijft over de risico's van informatie in de cloud. Wanneer bedrijfsinformatie aan de cloud wordt toevertrouwd is er maar één strategie dat een bedrijf kan toepassen om zich te verzekeren dat de vertrouwelijkheid en integriteit van die informatie geborgd is: vercijfer je informatie vóór je het aan de cloud toevertrouwd. Hierbij is het belangrijk om de vercijfering op bestandsniveau te doen, in plaats van vercijfering van het datakanaal.

By: Joe Sturonas. Joe Sturonas is Chief Technology Officer for PKWARE. PKWARE offers software solutions to critical IT problems, namely the explosive growth of data, the need to secure data, and the emergence of data in the cloud. He can be reached at Joe.sturonas@pkware.com.

As the proliferation of data continues to plague businesses, the pressure is on for companies to migrate away from their physical data centers usually on premise or within rented cages at large hosting providers. Cloud computing is being adopted at a rapid rate because it addresses not only the costs for physical space but also rising energy costs and mandates for more scalable IT services. Enterprises are drastically reducing their storage spend by using online storage solution providers to store massive amounts of data on third party servers. The trend of skyrocketing adoption rates for cloud computing is largely due to the more flexible on-demand IT resource capabilities, allowing anyone to capitalize on scalable storage solutions. According to IDC, public IT cloud services spending is expected to reach $72.9 Billion in 2015. Likewise, Gartner estimates that enterprises will spend $112 billion by 2015 cumulatively on cloud related technologies. The cloud is definitely calling, but even the most seasoned IT professionals debate, grapple and even get a bit intimidated by an otherwise simple term that has taken the world by storm.

Defining the Cloud

For professional collaboration and a more technical understanding, it is useful to standardize our definitions. Leveraging the Cloud Security Alliance [1] and published work of the scientists at the U.S. National Institute of Standards and Technology and their efforts around defining cloud computing [2] we find:

"Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable resources (e.g., networks, servers, storage, applications, and services). Cloud computing is a disruptive technology that has the potential to enhance collaboration, agility, scaling, and availability, and provides the opportunities for cost reduction through optimized and efficient computing. The cloud model envisages a world where components can be rapidly orchestrated, provisioned, implemented and decommissioned and scaled up or down to provide an on-demand utility-like model of allocation and consumption."

> Any clouds are at high risk for loss, breach and exposure

If we explore even further, Cloud computing is often divided into three main service types: Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS). And by design, each impacts data control and governance in a slightly different manner. Since one of the most attractive features of cloud computing is efficiency afforded by economies of scale, the very inclusion of a blanket security protocol is perceived as restrictive and a possible deterrent to the masses.

> Cloud providers cannot help your damaged reputation

With IaaS, the customer may have full control of the actual server configuration granting them more risk management control over the environment and data. In fact, oftentimes IaaS or infrastructure Cloud environments will basically push all of the security protection onto the customer. In PaaS, the provider manages the hardware and underlying operating system but securing the applications developed against the platform and developing them securely belong to the consumer. With SaaS, both the platform and the infrastructure are fully managed by the cloud provider; security controls and their scope are negotiated into the contracts for

service. Amazon Web Services contract proves the necessity for security controls: it explicitly calls out encryption as an option for protecting "your Content", however Amazon does not provide it.

Lastly, the Cloud is generally categorized into three deployment models:

1. **Private cloud-** infrastructure is provisioned for exclusive use by a single organization comprising multiple consumers.
2. **Public cloud-** infrastructure is provisioned for open use by the general public. It may be owned, managed, and operated by a business, academic, or government organization, or some combination of them. It exists on the premises of the cloud provider.
3. **Hybrid cloud-** infrastructure is a composition of two or more distinct cloud infrastructures. (Source: NIST)

With a more complete understanding, we can now highlight several significant benefits of cloud computing:

- Replacement of capital expenses with operating expenses
- Reduction in hardware costs
- Less required capacity
- Lower technology risk
- Increased productivity
- Improved user experience
- Overall impact on the environment improved

"For the foreseeable future, Cloud computing and storage will be the primary means to automate routine tasks and provision for the flexible delivery of content when and where it is needed. As organizations get swept up in the benefits, they should stay vigilant –private, public, hybrid, any clouds are at high risk for loss, breach and exposure if data isn't properly protected."
~Joe Sturonas, CTO, PKWARE

In Practice: Sending Server Data to the Cloud
Enterprises are constantly dealing with ever expanding unstructured data, where Network Attached Storage (NAS) ends up being a dumping ground for unstructured data. When unstructured enterprise data needs to be archived for compliance and regulatory concerns, data centers are looking to do that on the least expensive storage they can, as there are few performance requirements on archive data. A simpler, less expensive and more reliable way to archive server data would be to compress and encrypt the data on the server before sending to the cloud.

In Practice: Sending Mainframe Data to the Cloud
IBM Mainframe data is stored in a disk organization known as a Count-key-data (CKD) architecture, which gets its name from the record format, where the disk is addressable through Cylinder-Head-Record, unlike open systems disk architectures where they are based on organizing the disk into sectors or blocks. In other words, IBM Mainframe files are very structured and require the files to be pre-allocated on disk before data can be written; and the record lengths, block sizes and space need to be known when allocated. Mainframe data files can be saved on less expensive Cloud storage, but the mainframe data will lose the structure it had as a CKD file. If the archive data needs to be restored back on mainframe CKD storage, the file will need to be pre-allocated with very specific record size, block size, data set organization (type of mainframe file) and maximum space allocation. Then the data would need to be transformed back as a mainframe file. A much simpler, safer and more reliable way to archive mainframe data would be to compress and encrypt the data on the mainframe before archiving to the cloud.

Inevitable Risk
Every minute of every day presents the opportunity for a data mishap. A security breach, as well as lost, stolen or even compromised records triggers negative exposure that quickly equates to forfeited sales, legal fees, disclosure expenses and a host of remediation costs. The fallout can result in years of struggle to recoup reputation and repair a brand in the marketplace. Cloud providers do not want to be held liable for any issues related to your data loss. Best case, they will credit back your fees, but nothing can help a damaged reputation or customers who leave your organization when a data breach occurs.

While the cloud environment seems be to a holy grail for trends around data proliferation and massive storage needs; clouds present complex security issues and put critical corporate data, intellectual property, customer information, and PII (Personally Identifiable Information) in potential jeopardy. Enterprises forfeit security and governance control when data is handed over and cloud providers do not assume responsibility.

The recent cyber attacks and associated data breaches of Google and Epsilon (a leading marketing services firm) illustrate the need to incorporate an advanced risk and compliance plan that includes any third-party managed cloud environment. Clearly, the cloud often opens a Pandora's Box for unanticipated consequences.

Storing huge amounts of data on third party servers may mean instant online access and lower costs; however, that data is often comingled on shared

servers and exposed to users you don't know. If your Cloud storage provider encrypts your data but holds the key, anyone working for that Cloud storage provider can gain access to your data. That means the potential of your data be shared, sold, marketed to and profiled for someone else's gain.

Any data stored in dormant VMs lacks protection

Data also has to actually "get to" the cloud, which usually means leaving your trusted infrastructure and overcoming compounded transfer vulnerabilities as data moves to and from the cloud. Even the most unintended data breach could cost a company its reputation.

Potential Pitfalls

Transfer vulnerabilities - The potential for data breaches is multiplied as data travels to and from the cloud using various networks especially in highly mobile and distributed workforces.

Non-compliance penalties - Extended enterprises, partner networks and virtual machines are continuously scrutinized for compliance. All sensitive data must be protected with appropriate measures.

Storage expense - Companies are charged by the amount of data that is put into the cloud; therefore providers lack motivation to compress that data. Any compression by providers is deemed unreliable since encrypted data cannot be compressed.

VM control - Sensitive data that is transferred to an unprotected virtual machine (VM) will be exposed to users with access to the shared server. Any data stored in dormant VMs lacks protection when the operating system is not active or properly patched. VM sprawl wastes resources and creates unmonitored servers that could have access to sensitive data.

Provider holds the keys - Cloud agreements can address how internal folks at the vendor will be managing your data. Provisions can limit administrative access and grant who has hiring and oversight over those privileged administrators. If the data that is housed in the Cloud is, in fact, encrypted then the issue becomes more about who maintains the keys.

To summarize…

Security breaches will happen even for the most vigilant that do not encrypt their data.

Your company's reputation is at stake.

Security regulations are increasing.

The Cloud introduces new levels of risk.

Unsecure services, such as Dropbox, pose a security risk

Cloud providers have root access to all your unencrypted data in the cloud, and they are not your employees.

The only way to protect data in the cloud is if you encrypt the data and you maintain control of the private key.

CLOUD SECURITY BEST PRACTICES

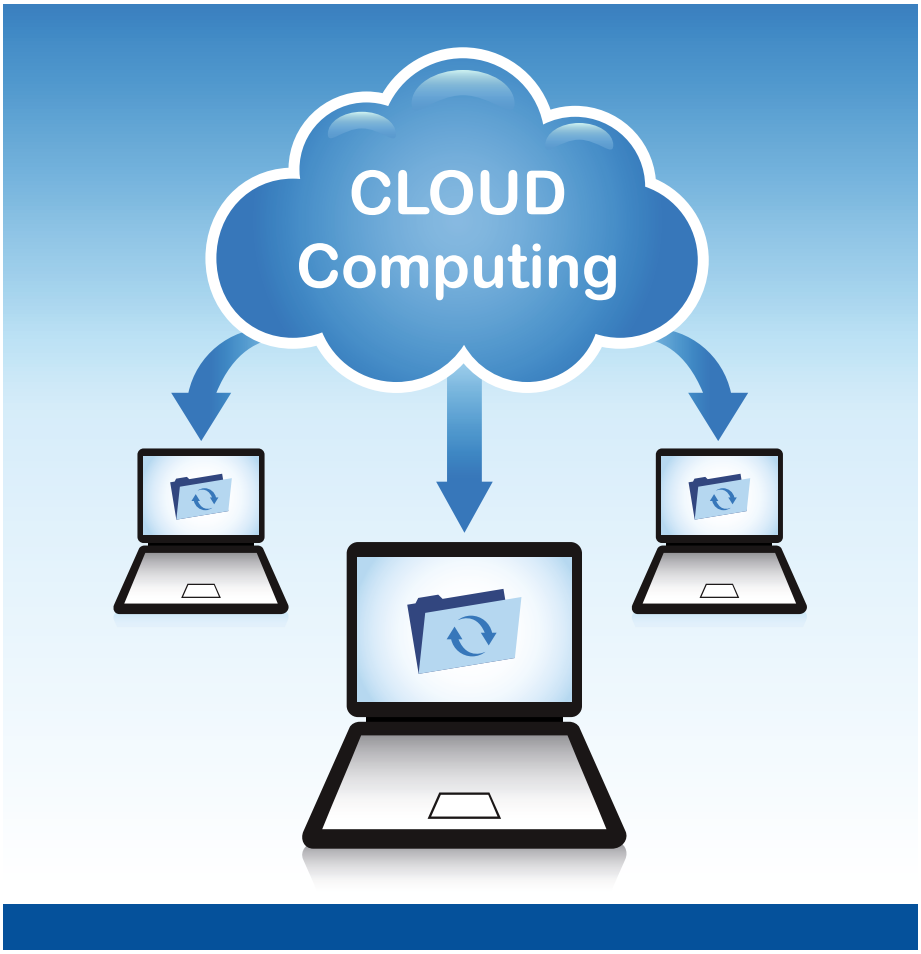
Impact on security policies and procedures?

Your existing security policies and procedures need to be reviewed to evaluate the use of Cloud applications and storage. Some companies choose to shut off access to certain Cloud applications, some choose to implement application-stores to limit access to specific approved applications, and some do not attempt to curtail access at all. Shutting off access is not a popular option to your employees who are most likely already familiar with consumer type options, such as Dropbox. Your end-users have certain problems like transferring or sharing a large file too large for email that they know such services can solve.

Employees, internal team members and partners, may not have any idea of the risk of putting data in the Cloud insecurely. They probably have no idea that unsecure services, such as Dropbox, pose a security risk and may have sensitive company data stored there. You need to alert them to the data security risks of the Cloud and have them sign a security policy to that effect.

The regulatory standards issues that you deal with today in your own data center are just as important in the

Cloud. Compliance with PCI DSS, EU Privacy Act, Sarbanes-Oxley, and FIPS140-2, etc. are just as imperative. If you know that the data is encrypted before it goes into the Cloud, you may be compliant with any number of these regulations. Even if the Cloud vendor is hacked or someone uses an administrative password improperly, your data is impregnable at that location.



EVALUATING SECURITY SOLUTIONS FOR THE CLOUD

Encrypting your data and maintaining the keys yourself is considered by industry experts as the only way of making sure that no one can read your data, period. It doesn't matter if a privileged user has access to your data, they still can't decipher it.

According to Cloud Security Alliance's "The Security Guidance for Critical Areas of Focus in Cloud Computing" [3], one important way to increase data protection, confidentiality and integrity is to ensure that the data is protected in transit and at rest within the cloud using file-level encryption. It points out, "encryption offers the benefits of minimum reliance on the cloud service provider and lack of dependence on detection of operational failure."

Regulatory compliance counts in any cloud, any environment, any country, you must ensure your data is compliant with any regulation standards for your industry.

If there are assistants, executive and sales representatives who use different operating systems on different computing platforms and want to share that data securely inside or outside of the private or public cloud…then you need data-centric, file-level encryption that is portable across all.

Be sure to evaluate Data Location and Data Segregation as they relate to co-tenancy. Not only do you want to hold the key, but you want to encrypt all of your data so that your data, especially sensitive data (PII), is protected if comingled with other organization's data.

A Cloud security solution must also enable recovery and provide you with the ability to restore your data many years from now. To meet some regulatory compliance statutes you have to keep your data for seven, even 20 years.

Cloud providers might assure users that the communications from your browser to their servers are encrypted using TLS. That provides a level of protection of the data only as it travels through the Internet, but then data remains in the clear once it landed on their server.

> You will have to report a breach one day

Worry-free breach

Odds are you will have to report a breach one day. If that day comes, you want to announce that no data was compromised and minimize corporate liability both in dollars and reputation. With data-centric encryption where you hold the keys and the data is encrypted at the file level, no one can access that data. Therefore, you may not even have to report it as a breach and you don't really have to rely on all the remediation contractual issues…because essentially there was a breach but no data was lost.

So before you store sensitive data in the Cloud, make sure you encrypt that data. This insures that your data is safe and accessible to you and only you.

References:

Cloud Security Alliance: http://www.cloudsecurityalliance.org

U.S. National Institute of Standards and Technology: http://www.csrc.nist.gov

Cloud Security Alliance's "The Security Guidance for Critical Areas of Focus in Cloud Computing": https://cloudsecurityalliance.org/research/