

# Protecting Trade Secrets in the Cloud

HONIGMAN

## Article By

[Nicholas A. Gowen](#)

[Honigman Miller Schwartz and Cohn LLP](#)

## Related Practices & Jurisdictions

- [Antitrust & Trade Regulation](#)
- [Corporate & Business Organizations](#)
- [Communications, Media & Internet](#)
- [Administrative & Regulatory](#)
  
- [All Federal](#)

Monday, October 20, 2014

The business community's growing use of cloud-based computing services provides great benefits due to cost-savings and mobile information access. However, business leaders should understand the risks of storing valuable trade secrets in the cloud. This article provides the business community tips on how to safeguard valuable trade secrets stored in the cloud from being freely disclosed to the public, thus putting the business at risk of losing protections that courts grant trade secrets.

As businesses' profit margins have continued to shrink since the Great Recession, more companies have looked to reduce costs by reducing growing expenses related to their information technology departments.<sup>[1]</sup> The first line item to draw attention in the IT budget is frequently the rising costs associated with maintaining and upgrading system hardware. Businesses often find that housing and operating multiple servers stretches IT budgets thin by increasing maintenance, labor, and operational costs. The solution so many businesses have turned to is to move their valuable data to virtual servers, or the "cloud."<sup>[2]</sup> A recent survey of IT executives provides that companies will triple their IT spending on cloud-based services in

2014 over 2011.<sup>[3]</sup> Cloud service providers have also seen demand increase as they increase their cloud capabilities.<sup>[4]</sup>

Although cloud-based servers provide businesses with substantial financial and operational benefits, businesses must recognize that there are perils to shifting data to the cloud. One of the key concerns businesses should consider before moving data to the cloud is the risk that its valuable trade secrets will lose protection as a result of insufficient safeguards to protect against disclosure. This article addresses that concern and provides businesses keys for seeking to protect valuable secrets in the cloud.

## **What is a Protectable Trade Secret**

The initial step for a business to determine how to protect its trade secrets is to understand how the law characterizes a trade secret. Information qualifies as a trade secret only if it derives independent economic value as a result of not being generally known or readily ascertainable, and be subject to reasonable efforts to maintain its secrecy. Trade secrets are broadly defined as information, including technical or non-technical data, a formula, pattern, compilation, program, device, method, technique, drawing, process, financial data, strategies, pricing information, and lists of customers, prospective customers, and suppliers.

## **Businesses Need to Take Reasonable Efforts to Protect Trade Secrets in the Cloud**

Trade secrets are only protectable when the owner takes reasonable efforts to prevent them from being freely disclosed to the public so that the information does not become generally known.

Information does not have to be cloaked in absolute secrecy to be a trade secret, as long as a business's efforts to maintain secrecy or confidentiality are reasonable. It is easy for one to imagine how a business may protect confidential documents that are stored locally. Computer files may be password-protected with several layers of encryption software, with access limited to specified personnel. Similarly, paper files may be stored in locked cabinets, in secured rooms, where only specified personnel are granted access.

However, those seemingly straight-forward security protocols become murky when information is stored in the cloud. Unlike storing data on local servers, storing data in the cloud requires the owner to disclose confidential information to a third-party vendor. In most situations, disclosing data to a third-party eliminates trade secret protections. Therefore, businesses must take additional steps to ensure that its data remains secure.

## **Three Keys to Protecting Trade Secrets Stored in the Cloud**

There are no fail-safe measures to protect data stored in the cloud. The best way for a business to protect its trade secrets is to locally store and protect its most valuable data with the proper data security protocols. A business, however, should

not fear the cloud as long as it takes certain steps to ensure that it exercises reasonable efforts to protect its cloud-based data.

First, business leaders must conduct appropriate due diligence before selecting a cloud-provider. The business should conduct necessary research to select a reputable, well-established company that has the physical and technological capabilities to store and protect data.

Conducting due diligence on a provider includes ensuring that the provider has taken necessary steps to establish appropriate physical and virtual security protocols to protect the confidentiality of your information. Inquire how the provider establishes physical security measures, and monitoring capabilities to prevent unauthorized access to its data centers and infrastructure. Also, learn how the provider limits its employees' access to customer data and determine the internal controls that the provider has in place to prevent unauthorized viewing, copying, or emailing of customer information.

A business should also inquire about the provider's virtual security protocols. A business must generally understand how its cloud-provider's encryption software and security management systems work to protect data. If your business is not capable of independently evaluating whether the provider has proper security protocols, a good indicator is to ask the provider for its client list. If the provider has clients that are typically security-conscious companies, such as financial institutions or healthcare facilities, that is a good indication that the provider has been vetted and it has proper security measures in place. Finally, the provider should maintain sufficient data-protection insurance coverage to protect against potential data breaches or system failures.

Second, a business must have contractual safeguards in place with its cloud-provider to adequately protect its intellectual property and trade secrets. The contract should establish that the business owns the data, that it will be segregated from other data groups, and that the business may enjoy unfettered access to the data. The contract should specify that the business can demand that the data be deleted or returned request, and detail how the provider will purge the data to ensure that it is properly deleted upon termination of the relationship. The contract should require regular data backup and recovery tests, while restricting the provider from accessing, using or copying data for its own purpose. Finally, the contract should establish the provider's obligations to notify the business of a data breach or system failure.

Third, a business should also consider adding multiple layers of authentication and encryption to data containing trade secrets before transmitting it to the cloud-provider. However, a business should consider if the additional encryption efforts could adversely affect the business's ability to access, utilize, and port data for its normal business use.

## **Conclusion**

There are several financial and operational benefits for a business to store data in the cloud. However, businesses must understand that there are also risks to storing its valuable trade secrets on virtual servers. Businesses need to take reasonable

efforts to protect the confidentiality and secrecy of its most valuable data and information.

---

[1] Dave Rosenberg. Reducing IT Infrastructure Costs via Outsourcing. May 7, 2009. [news.cnet.com/8301-13846\\_3-10235742-62.html](http://news.cnet.com/8301-13846_3-10235742-62.html)

[2] Thor Olavsrud. How Cloud Computing Helps Cut Costs, Boost Profits. March 12, 2013. [www.cio.com/article/730036/How\\_Cloud\\_Computing\\_Helps\\_Cut\\_Costs\\_Boost\\_Profits](http://www.cio.com/article/730036/How_Cloud_Computing_Helps_Cut_Costs_Boost_Profits)

[3] Andrew Horne. Transformational Change in IT Will Drive 2014 Spending. November 5, 2013. <http://blogs.wsj.com/cio/2013/11/05/transformational-change-in-it-will-drive-2014-spending/>

[4] IBM Commits \$1.2bn to Cloud Data Centre Expansion. January 17, 2014. [www.bbc.co.uk/news/business-25773266](http://www.bbc.co.uk/news/business-25773266)

© 2021 Honigman Miller Schwartz and Cohn LLP

---

National Law Review, Volume IV, Number 293

**Source URL:** <https://www.natlawreview.com/article/protecting-trade-secrets-cloud>