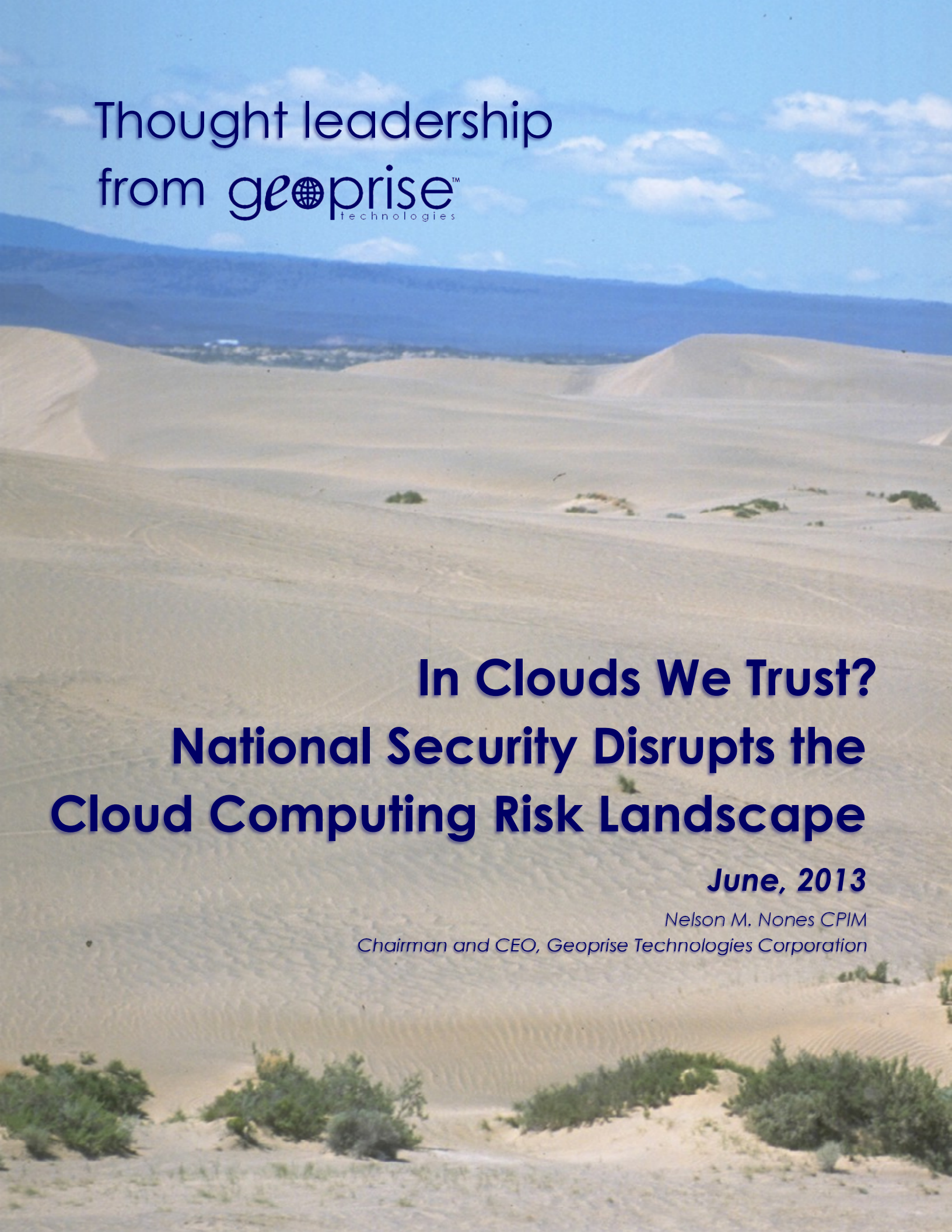

In Clouds We Trust? National Security Disrupts the Cloud Computing Risk Landscape

June, 2013

Nelson M. Nones CPIM
Chairman and CEO, Geoprise Technologies Corporation

A SUDDEN COLLAPSE OF TRUST THREATENS THE PUBLIC CLOUD COMPUTING INDUSTRY

In response to press reports on June 6th, 2013, the United States (US) government has essentially confirmed that it is secretly gathering massive amounts of Internet data, and both President Obama and the US Director of National Intelligence have since defended this practice vigorously. The sheer breadth and scale of US government surveillance makes it clear that using popular cloud computing offerings introduces much higher business risk than was ever generally understood before. These risks include:

- Financial penalties when doing business in countries having data protection laws;
- Financial penalties when processing data in countries having data protection laws;
- Business disruption when operating or processing data in countries having data protection laws;
- Data security breaches impairing private global commerce;
- Financial liability for data security breaches; and
- Reputational damage.

Businesses of all nationalities bear full responsibility for fulfilling their data security obligations, yet are powerless to block data leaks when using public cloud services. For many, lack of control over data security may overwhelm the public cloud's benefits.

Setting aside the furor over privacy threats to US individuals, we believe these risks also pose consequential threats to:

- Cloud service providers with data centers in the US;
- Their business customers of all nationalities who operate in countries having data protection laws;
- US businesses who outsource data processing to cloud service providers having data centers in countries where data protection laws are enforced;
- US businesses with customers outside the US; and
- Non-US businesses with customers in the US.

Geoprise believes these threats will be perceived to be so serious that many businesses could decide to abandon the use of cloud computing services going forward — or refuse to consider cloud computing at all — because they bear full responsibility for compliance yet now realize that they have little or no ability to control the attendant non-compliance risks when utilizing major cloud services providers. In view of recent revelations, the tantalizing cost savings and efficiencies from cloud computing may be overwhelmed by the financial, business continuity and reputational risks.

Likewise, many major information technology (IT) service providers are likely to re-consider the business case for offering cloud computing services. US-based providers are especially vulnerable because they are barred by court order from disclosing any information about government demands for data; hence their customers can no longer trust that their data is secure and compliant in the geographies where they do business. Non-US based providers will be less likely to invest in the US — the world's largest cloud computing market by any measure — due to the diminishing market opportunities.

Cloud computing, a once-promising industry touted as the Next Big Thing for corporate IT, may not survive in its present form.

As a result, public cloud computing — a once-promising industry touted as the Next Big Thing for corporate IT — may not survive, at least in its present form, because it has suddenly become clear that the financial and operational risks may far outweigh the business opportunities and benefits for providers and customers alike.

US GOVERNMENT CONFIRMS THE EXISTENCE OF INTERNET DATA GATHERING PROGRAMS

Press revelations on June 6th, 2013 that the US government is gathering massive amounts of Internet data from US service providers such as Microsoft (including Skype), Google (including Gmail), AOL and Apple — including actual electronic mail (email), chat, stored data, voice over Internet Protocol (VoIP), file transfer and video conferencing content — prompted James R. Clapper, US Director of National Intelligence, to issue this statement on June 6th, 2013:

> *"The* [press] *articles refer to collection of communications pursuant to* [an act] *that is designed to facilitate the acquisition of foreign intelligence information concerning non-US persons located outside the United States. Activities authorized by* [the act] *involve extensive procedures, specifically approved by the court, to ensure that only non-US persons outside the US are targeted ..."*

President Obama confirmed Clapper's statement the following day:

> *"With respect to the Internet and emails, this does not apply to US citizens, and it does not apply to people living in the United States.* [These programs] *do not involve reading the emails of US citizens or US residents."*

CLOUD PROVIDERS CAN TRANSFER CUSTOMER DATA TO AND FROM THE USA AT WILL

In our August 2012 article, Forecast for Asia: Partly Cloudy Computing, Chance of Mainstream Adoption,[1] Geoprise noted that "To assure service continuity, major providers operate so-called 'geo-redundant' data center networks. Their customers' data are replicated at many data centers, allowing fast changeover to an alternate data center if a customer's primary center goes down."

To illustrate, Microsoft's latest Online Services Use Rights terms[2] for its software-as-a-service (SaaS) offerings — including Office 365, a popular cloud computing service for small and medium businesses as well as large enterprises that includes email, chat, stored data, VoIP, file transfer and video conferencing capabilities — allow its customers' data to be "transferred, stored and processed in the United States or any other country in which Microsoft or its service providers maintain facilities." All Microsoft customers must consent to the transfer of personal data outside their country. For its cloud computing customers operating in the European Union (EU), Microsoft currently discloses that its primary and backup data centers are located in Europe but its backup data centers for those customers' user identities (Active Directory) and Global Address Book data are in the US.[3]

In our August 2012 article, Geoprise also noted that "data controllers" — businesses which operate in the European Union (EU), or process personal data using equipment situated in the EU — "cannot transfer [personal] data to a country outside the EU, unless that country's laws and regulations protect the rights of 'data subjects' as much as the EU Data Protection Directive … no matter where they are incorporated or operate." When using Microsoft cloud computing services, Microsoft's customers are the "data controllers" and Microsoft, in its Privacy and Compliance policy, is "essentially a subcontractor":[4]

> *"You, the customer, have ownership of your data and the responsibility under the law for making sure that we are following the rules and that it is legal for you to be sending personal data to us."*

---

[1] Available for download free of charge at http://www.geoprise.com

[2] Published April 2013, downloaded from http://www.microsoftvolumelicensing.com/DocumentSearch.aspx?Mode=3&DocumentTypeId=31

[3] Downloaded from http://www.microsoft.com/online/legal/v2/en-us/MOS_PTC_Geo_Boundaries.htm on June 9th, 2013

[4] Downloaded from http://www.microsoft.com/online/legal/v2/?docid=31&langid=en-us on June 9th, 2013

Another Compliance Conundrum

A fictitious medium-size enterprise has its headquarters in Singapore and subsidiaries in Germany and the US. To keep IT costs low, it uses Microsoft Office 365 SaaS for its corporate email, VoIP and video conferencing in all three countries. The service subscription is administered from the Singapore headquarters office.

- Microsoft's data centers for this company's Office 365 subscription are located in Hong Kong, Ireland, Singapore and the US.
- Currently, the enterprise has to comply with Singapore rules because it is incorporated in Singapore.
- It also has to comply with EU rules because it operates a subsidiary corporation in Germany, and the personal data it controls may be housed at Microsoft data centers in Ireland.
- Moreover the enterprise must comply with Hong Kong rules because the personal data it controls may be housed at a Microsoft data center in Hong Kong.
- The EU, Hong Kong and Singapore impose a duty of care on data controllers that protects data subjects of all nationalities, everywhere in the world, from damage caused by negligent handling of personal data. This includes a duty to prevent transfers of personal data to other countries that provide an inadequate level of protection.
- It is now known that the US government secretly compels US-based service providers to hand over their customers' Internet data, targeting non-US persons outside the US in particular.
- This practice exposes the enterprise to the risks of sanctions and financial penalties in Germany, Hong Kong, Ireland and Singapore in the event any data subject sustains damages from Microsoft's secret disclosure of personal data to the US government.
- Microsoft does not accept any responsibility or liability for such risks.
- The enterprise can control these risks only by cancelling its Office 365 subscription, or by spending more money to encrypt all e-mail, VoIP and video conferencing data when using Office 365.

Even though Microsoft customers are legally responsible for making sure Microsoft follows the rules, Microsoft will not notify them when customer data is actually transferred to a different country; the most it will do is notify customer administrators when it changes its primary and backup data center disclosures.[5]

It's also worth noting that the EU's definition of "data subjects" includes everyone, be they "non-US persons" or US citizens, no matter where they live.

In our August 2012 article, we further noted that the US "satisfies EU data protection requirements by virtue of accepted Safe Harbor Principles" but, according to Brian Honan, Board Member of the UK & Ireland Chapter of the Cloud Security Alliance:

> *"Many of the companies allegedly involved in* [the US government's collection of Internet data] *are part of the Safe Harbor program. The fact the* [US] *government is potentially accessing that data could place the European organisations* [sic] *in breach of EU Data Protection regulations."*[6]

IMPLICATIONS FOR BUSINESS AND ENTERPRISE USERS OF PUBLIC CLOUD COMPUTING SERVICES

From what has now been revealed and confirmed about the US government's Internet surveillance programs, Geoprise has identified six specific risks associated with business use of popular public cloud computing services:

Financial penalties when operating in countries having data protection laws: any local or US-based company that processes personal data utilizing cloud services hosted in the US is at risk when it has a presence in any of the 27 EU member states, plus Australia, Hong Kong, Iceland, India, Japan, Korea, Liechtenstein, Macau, Malaysia, New Zealand, Norway, Singapore, the Philippines and Taiwan. Some exceptions exist; for example, Australia's rules apply only to locally-incorporated businesses, Japan's apply only to larger organizations, and the Philippines excludes personal data collected from non-residents. Penalties can be severe. In Ireland, for example, fines as large as 250,000 Euro (USD 330,000) can be assessed against a corporation.[7]

[5] Downloaded from http://www.microsoft.com/online/legal/v2/en-us/MOS_PTC_Geo_Boundaries.htm on June 9th, 2013

[6] *Forbes*, "NSA Surveillance Threatens US Competitiveness", June 7th, 2013. Downloaded from http://www.forbes.com/sites/richardstiennon/2013/06/07/nsa-surveillance-threatens-us-competitiveness/

[7] Downloaded from http://www.dataprotection.ie/ViewDoc.asp?fn=/documents/legal/4e.htm&CatID=23&m=e

Financial penalties when processing data in countries having data protection laws: even if a company doesn't operate there, it must comply if its cloud services provider processes its personal data utilizing equipment located in that country. The risk of penalties arises if and when the data is transferred to a US data center, or to any other country that provides less protection than the local rules and regulations. In this event any company, US-based or not, is potentially at risk in any of the 27 EU member states, plus Hong Kong, Iceland, India, Liechtenstein, Macau, Malaysia, Norway, Singapore and Taiwan. Penalties can be just as severe as if operating in these countries.

Costs of business disruption when operating or processing data in countries having data protection laws: in lieu of financial penalties, EU authorities can order companies to forfeit or destroy data. The costs of such actions include not only outlays for replacing the data in a compliant way, but also the revenues and profits lost as a result of the sanction, to whatever extent the business relies on its cloud computing services to market and sell its products and services.

Data security breaches impairing private global commerce: even when local data protection laws do not apply, most business-to-business transactions are governed by confidentiality agreements protecting trade secrets, intellectual property and sensitive data that would clearly be compromised by secret US government surveillance. For example, most businesses commonly exchange sensitive data via email, file transfer, VoIP and video conferencing services. When either party utilizes public cloud computing services for email, file transfer, VoIP and video conferencing and its cloud provider's data centers are located in the US, it is now evident that the US government can obtain the content surreptitiously, and this risk appears considerably greater when one of the parties is located outside US territory. To mitigate the risks, businesses must either bear the added cost and complexity of encrypting the content, or they could set up and run their own private services. For VoIP and video conferencing services especially, the cost will be prohibitive for all but the largest firms.

Financial liability for data security breaches: many business confidentiality agreements expose suppliers to potential financial liabilities for liquidated as well as non-liquidated damages in the event of a data security breach. These liabilities could potentially invite financial ruin. If the potential losses are large enough, businesses will choose to forego the revenues and profits instead.

Damage to reputation: negative publicity resulting from penalties and sanctions imposed by the authorities in countries having data protection laws could have a substantial adverse impact on future revenue and profits.

It is equally clear that when processing personal information there is little, if anything, that most companies can do to control these risks, short of strong encryption or abandoning the use of major cloud computing services altogether. Only big multi-national companies have the clout to negotiate their own terms of service with major providers like Microsoft, or direct providers to process their data at specific locations.

IMPLICATIONS FOR PUBLIC CLOUD SERVICE PROVIDERS

Global public cloud service providers operate in a highly challenging market. To compete they must be able to keep their costs as low as possible while assuring high availability through service level agreements (SLAs) that offer full or partial credits if specific uptime commitments are not met. To manage SLA risks, they generally reserve the right to:

- Transfer a customer's data or processing to a backup data center without prior notice; and
- Require customers to prove compliance with a use rights policy before issuing refunds.

With respect to national data privacy laws, service providers generally mitigate their risk exposure by shifting the entire compliance burden to their customers, as our earlier Microsoft examples illustrate. Of competitive necessity this requires service providers to disclose the countries where their data centers are located, but their disclosures reflect a delicate trade-off:

- Disclosing too many location details invites security risks; yet
- Disclosing too few drives prospective customers to competitors who are more transparent.

From our observations during the past two years, Geoprise believes that the competitive environment is forcing most service providers to become more transparent when disclosing service locations, but providers are yielding to competitive pressures very reluctantly.

To this mix must now be added the need among US-based providers to comply with top-secret demands of the US government. Under US law, providers receive costs and full immunity from civil suits when they comply, but with the veil of secrecy lifted they can no longer shield themselves from customer scrutiny. Geoprise believes the erosion of customer trust poses an imminent threat to service providers because no US laws relieve *customers* of any obligations to comply with data protection mandates and covenants — only *providers* are entitled to financial consideration and immunity under present US law. Geoprise has identified two specific risks for public cloud service providers:

Loss of revenues and profits for US-based service providers: revenues and profits of US-based service providers will suffer to the extent that businesses of every nationality abandon the public cloud computing services they are now using, or refuse to consider public cloud computing services offered by US-based providers, in response to the heightened customer risks that have now been revealed.

Loss of growth opportunities for service providers worldwide: the US is by far the world's largest market for public cloud computing services. Gartner, an industry observer, estimated in February 2013 that the US market will account for nearly 60% of USD 367 billion in new worldwide spending on public cloud computing services (excluding cloud advertising) between 2013 and 2016, with new Western European spending placing a distant second at 25%.[8] That's equivalent to market demand averaging USD 72 billion per year of new revenues in the US, versus USD 29 billion per year in Western Europe and USD 21 billion throughout the rest of the world. But a rapid contraction of market demand caused by sudden loss of confidence in the security of US-based cloud computing services could cause the entire industry to re-think its growth targets and investment strategies, at least for the short to medium term, and in the longer term might motivate a fundamental restructuring of the business model upon which most public cloud computing services are built.

[8] Downloaded from http://www.gartner.com/newsroom/id/2352816

CONCLUSIONS AND RECOMMENDATIONS

Recent developments portend a sudden disruption of the cloud computing risk landscape that could extend well beyond the US to affect businesses throughout the world. As we noted at the beginning of this article, many cloud service providers with data centers in the US, their business customers who operate in countries having data protection laws, US businesses who outsource data processing to cloud service providers in those countries, US businesses with customers outside the US, and non-US businesses with customers in the US all face greater data security risks than they ever imagined before. In response, Geoprise believes they should conduct thorough risk assessments as quickly as possible to:

- Know and understand the implications of their commercial and personal data protection obligations in the countries where they do business. Geoprise has discovered that many of our clients are unaware of the rules they must follow or the penalties they might incur and, even when they are, the regulatory landscape is shifting rapidly. In Asia, for example, new laws were enacted only within the past year in the Philippines and Singapore, and existing laws were implemented or amended in Australia, Malaysia and Taiwan. The EU has announced revisions to its data privacy rules and regulations that are expected to take effect within the next two to three years, and could increase non-compliance penalties up to 2% of a company's worldwide revenues;
- Review terms of service, SLAs, use rights, data encryption practices and service locations for the public cloud services they currently utilize or are considering. This, too, is an ever-changing landscape due to the industry's rapid growth and competitive climate;
- Similarly review the service providers utilized by customers and suppliers with whom they exchange personal or sensitive data via email, VoIP, file transfer, video conferencing and similar services. Strengthening one's own IT security will have little effect if trading partners allow data to leak out;
- Re-calibrate their risk exposure from using public cloud services by rationally gauging the probability that service providers could secretly disclose personal or sensitive data to the US government without their knowledge or consent. The answer is by no means certain due to US government secrecy, but should take known factors into account such as data center locations, the degree of strong encryption utilized (rendering it difficult or impossible for the US government to decrypt) and the proportion of users who are non-US citizens. In view of the uncertainties Geoprise believes an extra contingency allowance would be prudent; and
- Identify new business controls, or revise existing controls, to bring them in line with the re-calibrated risk. If possible, re-negotiate service terms, encryption practices and permitted service locations with cloud service providers but this is a realistic option only for the largest businesses. Others will need to seriously consider curtailing their use of public cloud computing services if necessary, or switching to service providers who are situated beyond US government reach.

In view of recent developments, businesses should conduct thorough risk assessments covering their obligations under national data privacy laws as well as commercial contracts, their potential risk exposure from using US-based public cloud computing services, and the tools at their disposal to control the risks.

The outcomes of these risk assessments might cause them to curtail the use of public cloud computing services, or switch to service providers who are beyond US government reach.

ACRONYMS

EU: European Union
IT: information technology
SaaS: software as a service
SLA: service level agreement
US or **USA**: United States of America
USD: United States Dollars
VoIP: voice over Internet Protocol

www.geoprise.com

Corporate Headquarters

Geoprise Technologies Corporation
201 Norman Ridge Drive
Minneapolis, MN 55437-1709
USA

USA, Canada and Puerto Rico

Toll-free phone: 1 888 965 8868
Toll-free fax: 1 888 965 8868

Outside the USA, Canada and Puerto Rico

Phone: +1 310 209 8973
Fax: +1 310 209 8973

Asia-Pacific Headquarters

Geoprise Technologies Co., Ltd.

3F, 72/322 Moo 8, Rattanathibet Road
Bangkrasor, Muang, Nonthaburi 11000
THAILAND

Phone: +66 (0)2 965 8868
Fax: +66 (0)2 965 7761

ABOUT GEOPRISE TECHNOLOGIES

Geoprise Technologies was formed in 1999 by a group of software executives with over a century of previous cumulative experience building enterprise resources planning (ERP) and manufacturing operations management systems, and implementing them worldwide.

Our mission, then and now, is to create exceptional value for our customers by harnessing the power and economy of information technology to enable lean, world-class industrial operations on a global scale.

Today, Geoprise Technologies focuses exclusively on delivering top-quality expertise and technology solutions for businesses operating in Asia and the Pacific Rim, Europe and North America. We concentrate our expertise in two practice areas, strategy and operations and information technology, serving primarily the life sciences, energy and financial services sectors.

We deliver value with the utmost integrity by maintaining strict independence from other professional firms and technology providers, intense commitment to business ethics and profound respect for intellectual property rights.

DISCLAIMER

The material included in this publication is intended as a general guide only, and its applicability to specific situations will depend on the circumstances involved. You should not rely upon this information as legal advice or final advice. While we have made all reasonable attempts to verify the accuracy of the information contained herein as at the publication date, Geoprise Technologies accepts no responsibility for any errors or omissions it may contain, whether caused by negligence or otherwise. Neither does Geoprise Technologies accept any responsibility for any losses, however caused, sustained by any person that relies upon it.

Designed and produced at Geoprise, Thailand. Front cover photo credit: Bureau of Land Management/Oregon.