

The Official Magazine of the International Association of Outsourcing Professionals

# Globalization Today

July/August 2011

Commerce Redefined

## THE VENDOR VIEWPOINT

We survey the outsourcing vendor community on a host of vital issues that affect your business and career.



Also in this issue:

- *Disaster Preparedness: Getting it Right*
- *Innovation in Business Processing Outsourcing*
- *Protecting Privacy in the "Cloud"*



# Privacy Issues for the Cloud and Offshoring: **Solved**

In a June 29 editorial, “The Cloud Darkens,” the New York Times wrote: “The Internet is getting scary. In recent weeks, hackers known as Lulz Security attacked the Web sites of Sony, the United States Senate, the C.I.A., PBS, among others. ... A survey earlier this month by the Ponemon Institute found that 9 out of 10 companies had suffered an online attack in the last 12 months.”

The editorial went on to discuss how “Technology professionals are getting cold feet about moving more operations onto the cloud.”

If we are acutely vulnerable to attacks from outside, we seem to be doubly vulnerable to insider attacks. On the same day as the New York Times editorial, the Times of India published an article, “Indian IT, BPO face threat from insiders” which discussed a survey by PricewaterhouseCoopers and the Data Security Council of India.

“India’s growing outsourcing sector faces security threat from company insiders,” they reported. “Nearly 90% of all security breaches at 13 small, mid-sized and large IT/ITeS companies in 2009-10 was an insider job.”

What are governments doing to solve the problem? Unfortunately, their efforts may be making things worse. Privacy regulations such as those enacted by California and many European countries aim only to make security breaches extremely expensive for enterprises. For example, if a bank in California is hacked and its client data stolen, the firm would have to disclose that theft and make restitution to its clients. This could easily have a billion dollar impact on its market valuation. If however, the stolen data did not include information covered by privacy laws, the financial impact would be minimal. The intent of such laws is of

course to ensure that enterprises would be willing to spend appropriate amounts of money to protect their clients’ data.

Other regulations place restrictions on what companies can do with their client data. For example, France and Canada have restrictions on whether their citizens’ private data can be taken outside their national borders. Such regulations make offshore outsourcing impossible and force the creation of regional as opposed to global Cloud solutions. Some experts feel that such privacy regulations may in fact be a backdoor way to introduce barriers to global trade in services.

At the same time, developing economies that primarily act as the provider of global services may end up with restrictive regulations. Perhaps most notable are the recent data privacy rules enacted in India and the upcoming bill on the ‘right to privacy’ that is up for consideration by



the Indian Parliament. A Washington Post article, “India data privacy rules may be too strict for some U.S. companies” states, “Data privacy rules enacted last month in India are now alarming some U.S. companies, which worry that they may be too restrictive. ... Some [business leaders in India and the United States] say they are far more restrictive than American and European data privacy laws, and may put off customers.”

A Times of India article, “Govt to address US doubts about IT Act” expands on these concerns, stating: “legal experts and companies believe that under section 43A, an Indian IT/BPO company that enters into an outsourcing contract with, say, a US bank, would have to obtain written consent from each client of the bank whose information is sought to be collected. Such a consent requirement will potentially put a huge additional financial

burden on these companies and thus affect their profitability.”

Of course a significant source of these concerns is the fact that parts of Indian law are quite ambiguous and remain unclear. There is reason to believe that the regulations will be clarified and onerous regulatory constraints removed. In fact, the Washington Post article goes on to say, “India’s deputy minister for information technology Sachin Pilot dismissed the fears and said that the law addresses a long-pending demand of the IT industry for a legal framework for data protection. More than 2.8 million Indians work in the IT industry, and 9 million people are employed indirectly. ‘We are aligning ourselves with the global best practices. This law should end all the fears that any global company has about data being unprotected in India,’ Pilot said. ‘Why would we bring a law that will kill our sunrise industry?’”

The combination of the risk from hackers, the risk from insiders and the fragmented regulatory environment indeed seem to justify the title of the New York Times editorial. But is the Cloud really darkening? Are privacy concerns going to stymie the growth of Cloud Computing and Global Outsourcing? As countries like France and Canada continue to restrict the movement of privacy governed data outside their borders, will this lead to the growth of region or even country specific clouds instead of truly global Cloud Computing or outsourcing? For the editors of Globalization Today, this is an especially unwelcome prospect.

Albert Einstein famously said, “We can’t solve problems by using the same kind of thinking we used when we created them.” For fresh insight, we decided to reach out to Arijit Sengupta, the Chair of the Cloud Computing chapter of the International

Association of Outsourcing Professionals (IAOP).

A graduate of Stanford University and the Harvard Business School, and the lead inventor on seven patents related to outsourcing and Cloud Computing, Arijit is one of the most non-traditional thinkers around. In fact, the Silicon Valley based company he founded, BeyondCore, was selected the Most Innovative Cloud Provider of 2010 ahead of more than 150 firms.

When asked about the concerns raised by this article, Arijit flashed a big smile and said “Oh, we solved that one already.” He went on to describe the patented SplitSecure solution recently released by his company which was selected among the top three Cloud Infrastructure solutions at the GigaOm Structure conference.

Arijit explained that SplitSecure enables companies to fully realize the benefits of the Cloud and of Outsourcing by eliminating regulatory and security risks associated with processing privacy-sensitive data. Clients often refuse to outsource or Cloud-enable privacy-governed data due to concerns regarding privacy regulations. However, most information within privacy-governed documents does not actually need to be kept secure. Unnecessarily trying to secure the entire document prevents companies from adopting significant cost saving or strategic opportunities from outsourcing and Cloud Computing.

SplitSecure divides each transaction into multiple pieces so that each piece can be processed separately and securely. It determines the split after analyzing the

business transaction, such as a patient record, in light of all applicable constraints. These include (a) regulations and other information security rules, (b) processing rules that require access to certain combinations of information and (c) the relative effort required to process different fields.

SplitSecure then automatically splits out the maximum subset of information that can be safely placed in the Cloud or outsourced to a low cost location without violating any regulations or other information security constraints. The “split” is automatically optimized so that the most ‘effort’ is offshored or placed on the cloud.

For offshored transactions, the optimization may be based on the manual effort required to process different parts of the transaction and their relative frequency of occurrence. For Cloud-based storage the optimization may be based on the expected size of different fields of data as well as their expected frequency. After each piece of the split transaction is processed, it is then securely reassembled, avoiding any concerns about vulnerable data being mishandled.

SplitSecure can also automatically handle the interactions of multiple regulations as long as each individual regulation has been mapped in the system. If data collected from France is processed in Canada remotely from India, the combination of regulations can be automatically computed.


With traditional methods, an army of analysts would have to manually figure out how the regulations interacted and what

the combination of applicable regulations required. As regulations change, only the changes need to be mapped in the SplitSecure system and all corresponding impacts can be automatically figured out and applied.

Why does this matter? Recall the bank that was going to face a billion dollar risk if its privacy-governed client data was stolen. With SplitSecure, the same attack results in minimal impact. Arijit explained that “All SplitSecured information is as secure as the location where the mapping key and certain retained information is stored. This critical information is typically 10% of the overall data. As long as this 10% critical information is kept completely secure by the client, the remaining 90% can be placed on the cloud or provided to an offshore outsourcing provider without risking privacy regulations. Even if the less secure information is hacked or an insider at the outsourcing provider steals the information accessible to it, no privacy regulations are triggered.”

Thus, the bank never faces the billion dollar risk and can take the optimal financial decisions regarding outsourcing and Cloud Computing.

This technology would also enable BPO providers to split outsourced transactions such as credit card and loan application processing or insurance claims such that the majority of the work can be done in cheaper locations without violating privacy regulations. Analysts estimate that approximately \$50 billion of potentially offshore-able work has to be processed



within EU, Canada, etc. due to privacy regulations. Arijit claims that about 60-80% of this work could eventually be offshored to lower cost locations by using SplitSecure.

In a simplified example, a claim may contain (a) identity information such as first name, last name and an identity number such as Social Security Number, (b) medical information such as existing medical conditions, symptoms, diagnoses, and treatments, and (c) financial information such as fees, co-payment rules and insurance payouts for the specific patient till date.

The identity information may be kept confidential by the client and the medical information can be provided to an offshore provider for processing, whereas the financial information can be processed by an onshore provider if the relevant regulations so require. After the offshore provider confirms that the treatments were appropriate given the other medical information, and the onshore provider calculates the appropriate payment amount based on the financial information, the client can combine the two pieces of processed information and use them to process the claim.

Arijit claims that SplitSecure offers two key advantages over existing methods like tokenization that try to solve similar problems. First, it can automatically figure out the interactions between different relevant regulations in a case such as a French patient's data stored in a Canadian server being accessed from India. Second, it can automatically optimize the maximum

amount of work that can be placed on the cloud or offshored without triggering privacy regulations. Thus, a significantly greater proportion of the work can be placed on the cloud by SplitSecure as opposed to traditional solutions.

A recent article published in the Technology section of the New York Times, "BeyondCore Combines Compliance and the Cloud" concurs with at least part of his explanations: "Separating information to enable cloud-based processing has been around for a while — as anyone trying to process credit card transaction while complying with the PCI standard can attest to — but having that process automated via a SaaS product is fairly novel. The technology appears appealing to service providers that want to give customers as much flexibility as possible when it comes to choosing the right infrastructure for the job."

SplitSecure seems to have found a way to automatically ensure that offshored or cloud-enabled data processing would not trigger privacy regulations even if hacked or stolen by insiders. So, does SplitSecure solve the privacy problem? Either way, the key is that SplitSecure offers an alternative approach to solving the privacy problem: not merely more regulation, but smart technology.

As venture capitalists and other firms like BeyondCore start focusing on solving this key customer pain through technology, we feel encouraged that a comprehensive solution will indeed be achieved. Is the Cloud darkening? Even if it is, there is definitely a silver lining. ■