The Cloud – Is There a Silver Lining?

GUY BETAR
Senior Legal Counsel ANZ, TIBCO Software, Australia

Cloud computing in its various forms is well and truly entrenched in the global IT world, despite still being comparatively in its infancy. The range of offerings through the cloud will no doubt expand, and the take-up is likely to accelerate, given the perceived advantages to be gained from a cost and resource point of view. The “Cloud” has therefore become quite a buzz word, and there are a growing number of enterprises around the world offering a range of “Cloud” solutions. More and more businesses and corporations are either considering or taking up some form of Cloud solution.

In this context then, to embark on such a topic, it is essential to have a simple and common understanding of what is meant by “Cloud”. No doubt there are a wide variety of interpretations of this term, but for the purposes of this article I am using the term to mean the supply via the internet of:

a. Software applications as a service – Software applications are installed on the supplier’s machines and can be accessed via a web connection on demand, without the need to install the application on the users’ machines and/or servers; and/or
b. Platforms as a service – Operating systems are similarly made available through the internet, and/or
c. Infrastructure as a service – Amounting to making available an entire virtual computer(s) via internet facilities.

Each of these three forms of internet supply means that the software, computing platforms and virtual machines/data storage respectively supplied by another party are located somewhere remote from the users, and the users access them via the internet. In this paper I will use the term “Cloud Services” to cover all three of these scenarios.

Now that we have a reasonably simple statement of what “Cloud” encompasses, we can briefly review the common issues and concerns a potential purchaser/user ought to consider from the legal/contractual perspective, when looking at Cloud Services. This will provide the context for looking beyond those issues to the area of real focus of this article, which is to draw out some of the deeper considerations legal counsel and senior management should consider when looking at or acquiring Cloud Services. In doing so, I will principally look from the perspective of a purchaser of Cloud Services, not a supplier. This is not to say that purchasers of Cloud Services are the ones confronted with all the challenges – vendors also have issues of substance to address. However, the very nature of the business will mean that the number of purchasers of Cloud Services will for the foreseeable future far outweigh the number of suppliers, and hence the purchaser’s view of this paper. For convenience, a purchaser of Cloud Services will be referred to as a “Purchaser”. Suppliers of Cloud Services will be referred to as a “Supplier”.

In no particular order, the principal areas of contractual/”legal” concern for a Purchaser of Cloud Services are as follows. Opinion may vary as to other areas of concern, and this list is not intended to be exhaustive. The objective is to highlight many of the important
areas and to provide context for looking beyond the traditional “lawyer’s” view, to suggest additional considerations.

1. Privacy Obligations
2. Security
3. Access to data
4. Location and possible movement of data
5. Third party involvement – sub-contracting
6. Liability & Responsibility
7. Confidentiality
8. Statutory or industry specific requirements
9. Audit
10. Accountability of Performance
11. Business continuity
12. Termination
13. Dispute Resolution
14. Supplier Change

I will make some brief comments on the above issues, but before doing so, it is essential to re-emphasize the thrust of this paper. In considering the list of major concerns, the usual context of such consideration is the terms of supply offered by the Supplier, and to contrast that with what terms a Purchaser believes should be included in the contract of supply. It is largely about the contract, and seeking protection and assurance through the terms of the contract. This is of course essential and extremely important.

However, the key point which I will be expanding on throughout this paper is that consideration, negotiation and settlement of a contract is not the limit of activities and responsibilities for legal counsel concerning purchase of Cloud Services. Quite the contrary – legal counsel will need to interact with, brief, learn from and negotiate with, a variety of key people within their own company and possibly with outside organizations, including the Supplier. This is to ensure that not only is the Purchaser as well prepared as possible for using Cloud Services, but that the officers of the company who may be held responsible if things go wrong, are properly briefed and understand not just the potential benefits, but the downsides and risks, and what courses of action are available. An integral part of this particular review will be to look at just what might go wrong and the resulting ramifications.

We therefore must first briefly review the key issues that should be addressed in a contract for supply of Cloud Services. Some of the issues I have addressed in more detail than others. This reflects the nature of the issue and how challenging it may be in the context of Cloud Services:

1. Privacy Obligations –
   a. Privacy is a key concern for organizations and bodies in the private and public sectors throughout the world, and particularly for Cloud Services. Most developed countries have put in place legislation which seeks to protect personal information and privacy generally. The common understanding of personal information is information which identifies or is attached to the identity of, an individual.
   b. Purchasers of Cloud Services who have in their possession or control, personal information that falls within the Privacy regime of their territory, must ensure that in placing data containing such personal information with a Supplier of Cloud Services, the purchaser’s legal and policy Privacy obligations continue to be met through use of the Cloud Services. This will be a critical condition of
the contract for supply of Cloud Services, and the following additional issues should also be addressed in the contract with the Supplier:

i. The Supplier must be prohibited from itself using or “accessing” such data;

ii. The Supplier must facilitate, through the purchaser, access to individual data by the individual to whom the data relates (This may be technically and practically extremely difficult), subject to the particular laws of the applicable territory.

iii. The provisions of the agreement should extend to sub-contractors of the Supplier (See comments below on sub-contracting generally by a Supplier).

c. In paragraph (b) there is a deliberate reference to the privacy regime of the territory of the Purchaser of Cloud Services. A critical factor to consider in all Cloud Services scenarios is that once data goes into the “cloud”, it can potentially be affected by, or come within the jurisdiction of, one or more other territories, depending on where the data is stored (and this could be more than one location simultaneously), and where it might be moved to from time to time.

i. Therefore, it is not sufficient to only consider the legal regime of the territory in which the Purchaser resides. It is equally relevant (and not just for Privacy considerations) to look at the legal regime(s) of where the Supplier is situated, and where it stores data (which may be more than one place and may not be the same as where the Supplier itself is in fact located)

d. As with the majority of issues this paper addresses, considering them in the context of the supply contract, whilst essential, is by no means the limit of steps to be taken to address them, nor the extent of the perspective needed to comprehend the ambit of the challenge. This is considered more fully below.

2. Security

a. One of the critical questions to be asked, and then addressed in a contract for Cloud Services, is the level of security and encryption used by the Supplier to protect the data it will hold. This will necessarily involve technical staff on behalf of the Purchaser interrogating those of the Supplier to understand the precise nature of security measures and protocols employed.

b. Investigation into issues like physical media, location, redundancy, aggregation and related matters will need to be understood. In keeping with my point above, legal counsel should be aware of the need to investigate this issue, and should inquire into, and be kept informed as to, the results of the investigation.

c. A requirement should be imposed on the Supplier to destroy all data it holds for the purchaser of Cloud Services (after the Purchaser has obtained a copy of course), once the contract ends and the purchaser has recovered all its data.

d. Depending on the nature of the business carried on by the Purchaser, there may be special requirements (industry, legislative etc) to satisfy, such as having to segregate or isolate data. This needs to be specified and agreed.

3. Access to Data

a. A purchaser of Cloud Services may have either or both industry requirements and/or statutory obligations requiring it to give or facilitate third party access or possibly enable audit of, its data.

b. There are a variety of industries which are heavily regulated as to how they can collect, store, manage and deal with, data.
c. A further consideration might be access to the Supplier’s systems and facilities, and whether a right to audit the Supplier’s compliance with the agreement should be included in the contract. Such a right is considered below in the context of practical considerations concerning exercise of rights under Cloud Services contracts generally.

d. More particularly, as will be expanded upon below, such contractual rights may be of no real benefit as a literal access to the Supplier’s facilities and systems may not be feasible or practical – the data may be in one or more off-shore locations not readily accessible to the Purchaser.

4. Location & Movement of Data –
   a. The contract should strictly prohibit the Supplier from placing the data in any additional locations or moving the data to an alternate location or locations, without the prior written consent of the customer.

5. Sub-Contracting –
   a. The purchaser must know what entity or entities are supplying the Cloud Services, manage or are involved in the supply of the those services, and who has access to the data.

   b. This is particularly so where the Supplier is the primary business entity but it subcontracts to related or other entities in other jurisdictions. At the least the Purchaser (and legal counsel must be involved in this inquiry) should get a clear position on exactly how and where a Supplier does business, over what territories its business is spread, and what other entities are involved in delivering its Cloud Services. A Purchaser should have a contractual nexus to the entity or entities that control the data for or on behalf of the Supplier. If the Purchaser only has a contractual nexus with the Supplier (and the overall Cloud Services business of the Supplier involves other entities), then the multi-territory difficulties that could arise in trying to enforce rights against third parties with whom the Purchaser does not have a contract, could be impossible, even aside from the logistical challenges of geographic difficulties.

6. For Items 6 to 14, the issues should be self-evident, but some key points are as follows:
   a. Liability & Responsibility – This is linked to item 5 above. As with all IT type contracts, the interests of the Supplier and Purchaser are almost diametrically opposed. The Supplier will seek to minimize its liability and the consequences of its failure to meet its obligations. The Purchaser will seek to obtain as expansive a liability as it can impose on the Supplier, and for the Supplier to compensate it for as broad a range of loss as possible.

   b. In keeping with the tenor of this article, counsel for the Purchaser should look not only at traditional compensation for losses, but also additional more practical remedies. These should include providing access to facilities; delivering copies of stored data and security information to access the data.

   c. Traditional terms and conditions should by all means be included to deal with these issues, particularly tailored to address the nuances of Cloud Services. Further, in addition to rights and responsibilities, considered thought should go into what are the ramifications of having such rights, and what rights should flow from their breach.

Clearly all of these considerations are of importance in a contract for the supply of Cloud Services. However, looking beyond the terms of a Cloud Services contract will shed light on just how important it will be to understand the impact of what might literally happen,
and what courses of action a Purchaser of Cloud Services may have available when looking at and beyond the terms of a contract for the supply of Cloud Services.

Let us now consider some scenarios which are based on real facts. Consider a situation where the Supplier of Cloud Services with whom your company has contracted, is accused of (albeit unknowingly) having received data from or associated with, a terrorist group and/or harbouring (unknowingly) data related to international criminal activity. When doing due diligence on the Supplier, it was identified that their data storage and management facilities were located in a developed country which was deemed amenable to local or foreign orders, and therefore rights in and under your contract for supply of Cloud Services appeared likely to be enforceable. However, given the national/international security risks posed in this scenario, government security agencies of the territory where the data is stored step in and freeze the operations of the Supplier, pending further investigation.

Your company suddenly finds itself in a situation where through no fault on its part or indeed the Cloud Services provider, access to all data and facilities provided by the Supplier is suspended indefinitely. Because national/international security is involved, remedies against the Supplier are of no use. The statutory powers conferred on governmental bodies and agencies related to security and major criminal activity are extremely wide sweeping and under the former it is virtually without accountability. Ironically your company deliberately chose to go with a more expensive Supplier because all its infrastructure was in a developed country and therefore theoretically answerable to the jurisdiction of a sophisticated judicial system. However, where governmental authorities have stepped in this is not a civil matter and no amount of complaint to civil courts will likely assist. In particular, no matter what the contract with the Supplier says, and what rights your company might have, it will not assist you in gaining access to your data because the Supplier no longer has control over its infrastructure. Where matters of national security and/or serious crime are concerned, civil concerns will often have to wait in line.

If in such a scenario your company has taken up Cloud Services for mission critical support and/or retention of key business data, your company could be not only placed in jeopardy but so could its customers if they also rely on your company managing their data – consider a major financial institution, with credit card and trader account facilities. The potential damages sustained could be enormous and very difficult to contain. Looking again at the real thrust of this article – a Purchaser, through its legal and related management, must look beyond the traditional contractual approach for supply of Cloud Services, and consider additional rights and practical safeguards to minimize risk and exposure.

An additional and very important issue to take into account in this context, is what is the position of the senior officers of your company? Most developed jurisdictions around the world have some form of statutory and/or common law (or its equivalent) liability for corporate officers who fail to discharge their duties properly. In the fact scenario suggested above, what might the position of the senior officers of the Purchaser be if it was determined that insufficient precautions were taken to protect the company’s business and assets from such a set of circumstances. What precautions can in fact be taken? What might be determined to be reasonable precautions?

There is no one answer to these questions, and certainly no conclusive one. The letter of the law in different jurisdictions may have many different ways of addressing this topic, and the courts will likely arrive at quite different answers to the same question. Until such a scenario comes before the courts we will not know what the outcome might be. Even
then decisions may be confined to unique facts and/or law. What is critical here is to appreciate that to focus efforts on ensuring a favourable contract is agreed, and nothing more, is to potentially put both the company and its officers at considerable risk. My view is that it is essential to look beyond the contract to what might practically and literally happen, and appreciate how ineffectual the contract could be to deal with disastrous sets of circumstances. This in turn therefore begs the question – what else should or can be done?

Again there is no sure or definitive answer. However, my strong view is that there most definitely needs to be more done. So what might that be? Let us look more closely at the simple fact scenario described. When the company was seriously considering taking up Cloud Services, the following should have been carefully looked at:

a. What ongoing or regularly accessible technical back up or disaster recovery solutions does the company have, or might be able to acquire or implement, to safeguard from such a situation?
   i. Can you get regular (quarterly? Monthly? Annually?) complete copies of all the data from the Supplier. How and at what cost? The technical group must be involved to explore technical options with the Supplier and to ensure they will work. Once it is clear this can be done, then an obligation can be written into the contract.
   ii. How regularly should these be obtained to have a reasonable chance of recovering the majority of critical data. Can the importance of data be categorized and reflect actual access i.e. can critical data be physically accessed separately from non-critical, and thus copied much more regularly than non-critical?
   iii. Can the Purchaser directly access the data to back it up or must it rely on the Supplier providing the backup?
   iv. In the context of all these possibilities, what, if any, additional equipment, software, resources or other additional assistance must the Purchaser obtain or acquire to make them work, and what is the cost?

b. Such solutions must be at least partly independent of the Supplier of the Cloud Services – It is of no use for the Cloud Service provider to have backup and/or disaster recovery if you cannot access it.

c. As part of this consideration, what steps does a Purchaser have to take or have in place, to have access to the applications that utilize and run such data – for example if you are using software as a service from a Cloud Services provider, you need to have emergency access to the actual software and not just the data. This need expands to include systems and possibly hardware if your company used Cloud Services for platforms and/or virtual computers.

d. An accurate costing and budget needs to be done in parallel with these inquiries. This is essential so that those who must make informed decisions about not just what Cloud Services solution to take up, but what additional facilities and/or resources should be acquired and implemented. They can then make an informed decision about what level of risk to assume and at what cost.

Let us pause a moment to consider the implications of what is being suggested. In one view, these recommendations to an extent contradict the whole rationale of using Cloud Services. What is the point of trying to save money by utilizing Cloud Services, if you have to incur more costs with additional backup and other solutions that may have a major adverse impact on the cost savings? The point is that the costs savings may have a significant risk factor if taken literally without precautions. The real saving is a “net” one
and this should be clearly understood with all cost cuts and additional costs balanced properly.

It might be that the fact scenario proposed is considered a little extreme (though I can assure you it is not). Alternatively, in a varied scenario let us consider where the Supplier, or its data repositories, is/are not within a jurisdiction that affords authorities the rights to take control of such facilities and data. What then? For cost reasons (and again this is one of the underlying factors that makes Cloud Services attractive), the Supplier’s data facilities are not within your company’s territory. You negotiate rights to not only have access to the data, but literal access to the Supplier’s premises and equipment in the event of a breach on the part of the Supplier. The Supplier has contractually stated that its data storage is in a specified territory and your inquiries indicate this is correct, and that you would be able to enforce the contract within that territory. On this basis, you could reasonably feel that the major risks had been considered and addressed. However, without any warning, the Supplier shuts down its business and does not communicate with you. When you make attempts to contact the Supplier at the specified premises, you are advised the Supplier moved all its customers’ data to another location in a completely different territory under the custody of an entity constituted in another country. In this situation, the best contract in the world will be of no practical use whatever. It is with an entity that may or may not still be in existence, but worse still, that is not the same entity that now has control of your data. Even if you do know or find out where the data has been moved to, you may have no rights to access it in that territory, even if it is physically feasible to go to that territory to try to gain access the data. Further still, even if you were able to take formal steps against this new entity, it could take considerable time which may still leave your business crippled.

There are numerous permutations of this sort of fact scenario, all entirely plausible. If your company is investigating a Cloud based solution, or indeed seriously looking at one, then over and above settling a thorough and comprehensive agreement, what can legal counsel (and indeed all managers involved), do to minimize risks and have viable back-up solutions?

I recommend that legal counsel should take an active and dominant role in the investigation into the Supplier and its business, and overall assessment of the viability and risks of contracting for the supply of Cloud Services. This goes well beyond being responsible for just the contract. Legal counsel will be uniquely placed to:

1. Work with and co-ordinate the business unit(s) involved and possibly outside service providers, to investigate the Supplier and its business;
2. Similarly, work with and assist in the co-ordination of the technical inquiries about the Supplier’s services and solutions, and technical risk minimization measures and strategies the Purchaser can employ to reduce risks regarding data access and its retrieval;
3. Work with that part of the business responsible to put costs and budgets against the factors to be considered, then assisting to package up the entire proposal with all factors and costings, to enable senior management to make an informed decision.
4. Legal counsel should also provide guidance to those senior managers on the individual legal responsibilities of their role, and factors to consider in how best to discharge that responsibility. This must be considered not just in the light of business continuity, but also in the context of senior managers/officers being able to show they properly discharged all their duties.
In my view it is essential that the key tasks and several disciplines involved in the review and assessment process should not operate independently. Legal must have a continuing dialog with the technical management to understand what they want to implement and achieve through a Cloud solution. Further, legal must understand what technical options exist for back-up, risk minimization and safeguards. Non-technical management must also be involved in such dialogs so they equally understand the objectives and limitations, and the relevant cost impacts.

It will be critical for legal to emphasize to management that there will be limits to how much protection can be gained from contractual rights. There may be further limits depending on where the Supplier operates, and precisely what type of Cloud Service(s) is/are proposed to be used. If the Purchaser operates in an industry that is regulated in relation to data then this places further limits on how and where Cloud Services can be utilized.

If using Cloud Services is merely one of several redundancy strategies employed by the Purchaser, then arguably that is low to medium risk. If it is mission critical data, and the primary source of access to, manipulation of, and storage of such data, then the risk escalates substantially. The risk may be extended further where your company uses software as a service and therefore being exposed to losing the use of the software that manages the data as well as access to the data. The more dependence on the Cloud Services, the more the risk(s) may have gone through the roof.

One further consideration to keep in mind, is the extent to which insurance covers data and business conducted through Cloud Services. Where Cloud Services are being considered, the insurance policies in place should be reviewed carefully, and possibly specific questions raised with the companies providing the cover, to ensure that loss and liability insurance extends to cover Cloud Services. Senior management, particularly in the context of discharging their duties, will need to be informed on this matter so as to properly assess risk and the viability of the Cloud Services for their business.

Given the above, I feel it is very clear that for any company to seriously consider Cloud Services, they need to apply some key internal disciplines and strategies. The exact nature and extent of these strategies will vary a little depending on your company’s business, whether that business is regulated in such a way that it impacts how you must manage and protect your data, how widespread your operations are in terms of territories covered and affected, and the investigation and consideration of the Supplier in the ways and areas noted above.

As a minimum I recommend the following:

1. A team should be formed to consider and advise on, adoption of Cloud Services. That team should have a representative(s) from technical management, commercial management and legal.

2. Technical management should provide an outline of what specific Cloud Services are sought, what are the key reasons for looking at those solutions, and the cost/savings aspects.

3. Legal should outline the key areas of exposure for senior technical and general management, and this should include a succinct summary of exposures where contractual remedies are not likely to be of assistance or might not provide real or useful protection. Subject to the law or laws which apply to your company (i.e. there may be several bodies of law which apply depending on where your company trades and/or is sited, for
legal purposes), what responsibilities and duties apply to senior management that may have to be considered.

a. This advice should have an initial proviso that it is subject to the investigation of the Supplier yet to be completed, if it has not already been carried out.

b. It will also be subject to a review of the Supplier’s contract if that has not yet been done.

4. A person or persons should be designated to carry out a form of due diligence on the Supplier(s) being considered, with particular emphasis on where they are based, where they have their data storage and management facilities, do they use sub-contractors and/or related bodies, customer references, and what other jurisdictions, if any, they carry on business in.

5. Taking point 2 into account:
   a. Technical management should be asked to provide technical back-up and recovery solutions that will work on an ongoing basis in parallel with, or in concert with, Cloud Services, and which will address at a practical level the sorts of challenges identified in the risk scenario above and in particular the exposures.
   b. Legal should do a follow up set of points arising out of the due diligence carried out, and whether the information obtained from that inquiry impacts or changes the original advice given. Additional inquiry into the applicable laws of the relevant territories may be required.
      i. This follow up should include a review or assessment of the territories that will affect the taking up of Cloud Services, and a particular inquiry regarding data and privacy laws of those territories
      ii. This information then must be considered in light of where the Supplier operates and stores its (your) data. It is possible that several territories may be involved, and the laws of each one could apply to your company’s data either through the nexus of the Supplier itself, or the mere presence in the territory of actual data and/or equipment related to the handling of your data. (See point 8 below).

6. The solutions in 5 must have costs associated with them, including establishment (if any) and ongoing costs.

7. To properly assess the value and risks of securing Cloud Services the following must then be weighed against each other:
   a. The face value cost savings and other advantages sought to be gained from the Cloud Services;
   b. The content and strength of the contract, and whether it provides practical as well as “legal” protection.
   c. The costs of the back-up and alternate access facilities and strategies;
   d. Are there risks that cannot be covered by the back-up and alternate strategies and the contract, including assessment of insurance cover;
   e. As best can be reasonably determined, has as much been done to protect the company and its business as possible if the proposed Cloud Services are taken up?

8. As part of the assessment under point 7, the results of the inquiry under point 5(b)(ii) will be very important. It may be an expensive and time consuming process to obtain relevant and useful information about pertinent laws in the territories that are applicable. This is a decision which in itself must be made –
how much trouble should one go to and what level of expense should be incurred. Those with the relevant authority may well need to make decisions on the following:

a. If two or more territories are relevant to where the Supplier is and where it manages data, is it necessary or desirable to instruct local attorneys to advise on what local laws are applicable, and what affect they might have on your company’s data. In particular:
   i. What responsibilities, if any, fall on your company under such laws;
   ii. Might such laws have an adverse effect on other parts of your business – for example if your company’s data is held within a particular jurisdiction, does this constitute carrying on business or having a presence within that jurisdiction, either under your home territory law or the law of the other territories, which could have liability consequences and possibly adverse tax consequences.
   iii. Does the local law have comparable rights and obligations to the ones you are relying on under the contract. Would your contract with the Supplier be enforceable within that territory?
   iv. Is there an adverse effect or set of obligations placed on the management of your company, under such laws?

b. Those with responsibility for making decisions on whether or not to take up Cloud Services at all, and then with which particular vendor does your company go, have a potentially challenging time to consider all the factors and weigh risks.

9. Without wanting to sound overly dramatic, if the investigations and due diligence are carried out properly, and the practical risks of being able to access your data in the event something goes wrong are flagged, this will inevitably point to a risk scenario of some description. It is not a case of IF – but rather HOW MUCH. Quantifying risk is what business is all about. In this context, the cost savings are being balanced against the cost (both initial and ongoing) of risk reduction strategies, and the costs of seeking to enforce rights under a contract. Note these latter two costs are NOT the same thing.

a. It is also critical to note that the cost and risk assessment I am recommending is not confined to initial investigating and assessing a Supplier, before “signing up”.

b. It is equally critical, if not even more critical, to carry out regular update reviews on both the Supplier and how and where it carries on its Cloud Services business and particularly its data storage and manage activities.
   i. Key risk factors may change dramatically if:
      1. A Supplier is bought out or re-structures;
      2. A Supplier moves or splits its data storage and management to other or additional territories;
      3. A Supplier may become subject to claims or actions by third parties in one or more territories in which it carries on its activities, adversely affecting your company’s rights and/or abilities to retrieve or get access to its data.

c. A further element of change to keep in mind is that which affects the Purchaser. If changes in law alter the Purchaser’s data responsibilities these must be taken into account in its Cloud Services. A re-structure of the Purchaser or its group might equally have affects that need to be reflected in how it uses Cloud Services.
In conclusion, I suggest that Cloud Services have new and interesting challenges for legal counsel to identify and manage, and require a broader investigation and review by corporate counsel than most previously encountered new technology and/or services. The location issues and multi-territorial dynamics give rise to needs for looking at a variety of risk mitigation strategies understood by all senior management, particularly legal counsel.

So is there in fact a silver lining? That may have to await answer until use of Cloud Services is more mature and widespread and the upsides and downsides have played out in real scenarios.

Please feel free to contact me if you have any input on the subject, wish to discuss any of the issues or have any questions.

Guy Betar, Senior Legal Counsel ANZ – TIBCO Software, gbetar@tibco.com

***

Guy Betar is a Corporate/IT lawyer with over 20 years’ experience as a law firm partner, corporate counsel, and executive manager. His background is primarily as a corporate commercial lawyer, with specific international expertise in IT/IP, particularly technology and software. He has worked on transactions in various jurisdictions, from the Middle East, Europe and Asia to the US, and has negotiated and managed large, multi-national transactions in various parts of the world. He is very comfortable working almost anywhere in the world and has experience working professionally with a diverse range of cultures, laws and systems, including the Middle East, Asia Pacific, Europe and North America. He has extensive experience in advising on, structuring, negotiating, drafting and implementing complex commercial agreements and arrangements, particularly in the IP and IT fields. He is an experienced team leader, and well versed in executive management as well as the practice of law, and is a published author and an experienced presenter.

TIBCO Software Inc. (NASDAQ: TIBX) is a global leader in infrastructure and business intelligence software. With a broad mix of innovative products and services, TIBCO is the trusted, strategic technology partner of businesses around the world. www.TIBCO.com