RISKS AND BENEFITS OF BUSINESS INTELLIGENCE IN THE CLOUD

Christina Tamer¹, (617) 287-7720, christina.tamer@gmail.com
Mary Kiley¹, (617) 287-7720, mkiley265@yahoo.com
Noushin Ashrafi¹, (617) 287-7883, noushin.ashrafi@umb.edu
Jean-Pierre Kuilboer¹, (617) 287-7868, jeanjpierre.kuilboer@umb.edu

¹ University of Massachusetts Boston, Management Science and Information Systems
Department, 100 Morrissey Blvd,
Boston, MA, 02125 United States of America

ABSTRACT

The new phenomenon of business intelligence (BI) is transforming the way businesses handle data. BI environments require a large capital layout to implement and support the large volumes of data as well as massive processing power, which inflicts tremendous pressure on corporate resources. In recent years, cloud computing has made BI tools more accessible, but BI in the cloud comes with a number of risks and vulnerabilities; most notably threat to security. This paper presents the benefits and risks of using BI in the cloud and discusses the necessary precautions that should be taken prior to transitioning to cloud computing.

Keywords: business intelligence, cloud computing, risks and benefits, big data, saas.

INTRODUCTION

Traditional decision support systems have evolved to more complex solutions that support structured and unstructured data at all managerial levels and business processes [1]. Business intelligence (BI) refers to the organizational ability that captures internal and external information and converts them into knowledge. The assimilated knowledge is then used to develop new opportunities towards achieving competitive advantage. BI is indeed revolutionizing decision making and information technology across all industries. This phenomenon is largely due to the ever-increasing availability of data. The explosive volumes of data are available in both structured and unstructured formats, and are analyzed and processed to become information within context hence providing relevance, and purpose to the decision making process [2]. BI provides both information and knowledge that leverage a variety of data sources. Knowledge is derived from information but is more robust as it offers “justified beliefs about relationships relevant to the decision,” [2, p. 5]. BI enables decision makers to optimize business resources, increase efficiency, reach goals, and identify areas for growth. Reaping the core benefits of BI requires technical and conceptual integration, which, in turn, increases the complexity of data management and storage [3],[4]. The financial and organizational burden of BI solutions may easily override the benefits they offer. “In many cases, the integrated infrastructures that are subject to BI have become complex, costly, and inflexible.” [4]

Traditionally, Decision support systems tools reside on-premises. However, due to the increasingly digital presence of data [2 p. 262] many BI vendors are offering tools on the cloud. BI solutions based on Cloud Computing, called “Cloud BI” or “BI services on demand” are becoming increasingly popular and considered as one possible remedy to the restraints caused by BI solutions [4], [5], [2]. Cloud computing presents a model that provides
on demand access to software and hardware resources with minimal management efforts. The main features of cloud computing are: [6], [7], [8]

- Virtual, dynamic, scalable and massive infrastructure;
- Shared, configurable, flexible, dynamic resources;
- Accessible via internet from any device;
- Platform with minimal management or self-management;

The Cloud computing environment enables BI tools to be distributed as a service, more commonly known as Software as a Service (SaaS). SaaS is often called software “on demand” and has become a popular delivery model for business applications. Such models are data-centric and hosted in the cloud, making them accessible via a web browser. Most enterprise software companies now have several SaaS offerings on the cloud. SaaS is more robust and inclusive than Infrastructure as a Service (IaaS) or Platform as a Service (PaaS). Given the increasing popularity of cloud computing and the importance of choosing the appropriate BI tool, it is crucial to better understand the nature of cloud computing and examine the benefits and risks of using BI tools on the cloud.

Cloud computing is a virtual environment which gives users the facility to access computing power to which they might not otherwise have access due to financial or organizational limitations. Cloud computing, sometimes called “a field within service computing,” is a cross-discipline that bridges the gap between business and IT services. This discipline aims to enable IT services and computing technology to perform business services more efficiently and effectively [9]. In technical terms cloud computing includes service oriented architecture (SOA) and virtual applications of both hardware and software. Cloud computing shares its resources among a cloud of service consumers, partners, and vendors. By sharing resources at various levels, this platform offers various services, such as an infrastructure cloud, a software cloud, an application cloud and a business cloud [10]. For those of less technical backgrounds, the cloud is similar to a “computer co-op.” It enables entities to pool their resources to improve the business process at reduced capital costs. It also allows entities to outsource the information technology responsibilities, thus allowing the organization to focus on its core competencies. In essence, cloud computing provides large data centers at a low cost due to their expertise in organizing and provisioning computer resources.

While utilizing cloud computing delivers a number of benefits, enterprises that consider the use of the cloud in their environment should ponder upon the potential risks as well. Business must work with legal, security, and assurance professionals to ensure that the appropriate levels of security and privacy are achieved [6]. As pointed out by Gartner, “Organizations potentially gain a competitive or cost advantage through selective adoption of cloud computing, but not without first taking a comprehensive look at the associated risks, ensuring that they are consistent with business goals, along with the expectations of regulators, auditors, shareholders and partners. It is especially challenging to understand the risks associated with cloud computing ….” [9, page 2].

One of the biggest issues facing cloud computing is data security. For many mission-critical computations, cloud computing may be ill-advised because shared resource environment of cloud computing introduces unexpected side channels (passively observing information) and covert channels [11]. Other issues such as reputation fate sharing, which allows cloud users to take advantage of security best practices delivered by expertise at major cloud providers while at the same time a single disrupt can affect many users [12]. There is little doubt that
Cloud computing is viewed as a “target rich” environment for those wishing to do harm. Cloud users face security threats both from outside and inside the cloud. Many of the security issues involved in protecting clouds from outside threats are similar to those already facing large data centers. In the cloud, however, this responsibility is divided among potentially many parties, including the cloud users, the cloud vendor, and any third-party vendors that users rely on it for security-sensitive software or configurations.

In this paper we address benefits and risks of BI on the cloud and suggest some precautionary undertakings for organizations that would like to invest in cloud computing to achieve the ultimate goal of any modern business; gain economic advantage, but are weary of security risks.

The following sections discuss how cloud computing can improve BI, followed by what the main risks are. The discussion concludes with final considerations for managers when choosing a BI vendor and an overview of the implications for vendors themselves.

**BENEFITS OF BUSINESS INTELLIGENCE ON THE CLOUD**

When looking into practicalities of moving BI into the cloud we should first consider potential benefits and then examine the risks involved. In what follows we discuss the benefits.

**Increased Elastic Computing Power**
Computing power refers to how fast a machine or software can perform an operation. Hosting BI on the cloud means that the computing power, or processing power, depends on where the software itself is hosted, rather than the on-premises hardware. Cloud computing has become very popular over the last few years and is “hailed as revolutionizing IT, freeing corporations from large IT capital investments, and enabling them to plug into extremely powerful computing resources over the network,” [12]. As the volume of data increases to unprecedented levels and the growing trend of “Big Data,” becomes a norm rather than an exception more and more businesses are looking for BI solutions that can handle gigabytes (and eventually terabytes) of data [13].

The cloud lets users avoid the necessity to upgrade the computing power of their on-premise systems in order to use BI. Instead, it allows BI users to call on increased computing power as needed. The cloud’s flexibility allows BI users to instantly scale computing activities up or down depending on the project at hand [14]. This benefit of elastic computing power is advantageous in “the face of changing conditions,” [12]. Project sizes vary greatly and the flexibility in computing power is appealing for companies with fluctuating and growing data sources.

**Potential Cost Savings**
Pay-as-you-go computing power for BI tools has the potential to reduce costs. A user on the cloud only has to pay for whatever computing power is needed. Computing needs could vary considerably due to seasonal changes in demand or during high-growth phases [12]. This makes IT expenditure much more efficient.

The reduction of costs is particularly attractive for startups looking to use BI. Research by Gartner indicates that cost models can be cheaper over the first five years, as a direct
consequence of adopting the cloud. Long-term cost reductions are more difficult to quantify, but include the potential for reduced personnel costs and reduced IT support costs [15].

Regardless, any potential cost savings can be significantly beneficial to both BI vendors and users. For some vendors, cost is the “No. 1 reason that broader deployments [of BI are] blocked,” [16]. On the other hand, new and independent BI cloud vendors like LogiXML and Jaspersoft enjoyed good sales in recent years, with cost being the primary reason for customer adoption [17].

**Easy Deployment**
The cloud makes it easier for a company to adopt a BI solution and quickly experience the value. Managers will see results quickly and increased confidence surrounding the success of the implementation. Deployment requires less complicated upgrades for existing processes and IT infrastructure [18]. The development cycle is much shorter, meaning that the adoption of BI does not have to be a drawn out process, thanks to the elimination of “complicated upgrade processes and IT infrastructures demanded by on-premises BI solutions,”[15].

**Supportive of Nomadic Computing**
Nomadic computing is “the information systems support that provides computing and communication capabilities and services to users, as they move from place to place,” [19]. As globalization continues to dominate all industries, nomadic computing services and solutions will grow in demand. It also allows employees and BI users to travel without losing access to the tools.

The increasing number of global businesses, international offices, and remote teams, means that on-premises software can often be irrelevant or difficult to maintain. It is important for companies to use the same solutions internally, and it may be impossible to deploy the same on-premises solution across countries depending on the vendor. Globalized businesses will increasingly require BI solutions that are “more Web 2.0 and collaborative than Excel,” [13] in order to work effectively and uniformly across offices. The cloud makes it possible for a company to deploy a uniform solution around the world.

**RISKS OF BUSINESS INTELLIGENCE ON THE CLOUD**

Despite the numerous benefits of adopting cloud-based business intelligence, there are many risks. The following is a discussion of the risks cloud-based BI presents, with a particular emphasis on security.

**Security Risks**
Today, security and privacy may represent the biggest risks to moving services to external clouds [20]. According to a survey of Chief Information Officers and IT specialists, 75% of respondents consider security as the number one risk of cloud computing integration with BI [5]. Using BI on the cloud poses significant security risks. “Since BI and analytics are data-intensive, there [is] a lot of nervousness about relying on outside cloud providers handling massive amounts of corporate data,” [21]. With cloud computing, data is stored and delivered across the Internet. Since the location of data is unknown and not controlled by the owner of the data, there is a good chance that several competitors’ data and applications reside on the same resources environment. In this multi-tenant environment, it may be very difficult to
have the level of isolation and associated guarantees that are possible with an environment dedicated to a single customer [9].

As a result, there are many risks surrounding the loss or compromise of data. Data hosting may be untrusted or unsecure, with the potential for data leakage [22]. There is significant potential for a data breach or data loss, potentially compromising customer or otherwise confidential data. If there is potential for a data breach, an organization using cloud BI runs the risk of damaging the bottom line and its reputation [12].

As noted before, when putting data onto an external server and outside of the user’s direct control, there’s no way avoiding confidentiality risks” [23]. Encryption is a viable option, but it is the responsibility of the user to ensure that data is appropriately encrypted on the cloud. Any cloud technology require the process of virtualization: housing several different data sets and sources on a single piece of hardware. The practice of virtualization actually presents opportunities for highly technical security breaches, as data is stored forever, even when its index is deleted [22].

**Slow Data Breach Recovery**

When data is hosted outside a company’s direct control, the likelihood of a data breach remains high, but the recovery is more difficult due to the dependence on a third party. Timely and appropriate response to a data breach is crucial for customer retention. However, if the BI user does not know where the data is actually stored and processed (possibly outside the country), it is difficult to respond quickly, remedy the problem, and provide customers, clients, and employees with the answers they need in regards to privacy or accessibility.

**Cloud BI Availability Is Determined By External Factors**

Using BI on the cloud relies on the third party’s server availability, rather than on-premises availability. A user is “gambling that your data will be available when you need it when you put it in the cloud, betting that the availability won’t be eroded by network outages, data center outages and other single points of failure;” [23]. If there is a failure, the BI user could lose access, visibility or control of its data [22].

**Potential Compromise of Core BI Capabilities**

Traditional, on-premises BI solutions offer full control and high-touch data integration. Data integration capability, one of the four core BI capabilities, is crucial to defining a successful and robust BI solution. The cloud presents the potential for compromised data, metadata, and application integration, according to Boris Evelson of Information Management [13]. BI tools must offer the “capability to import/export metadata so that business and technical metadata can be integrated and reused with other enterprise applications,” [13]. Further, the import mechanism should be conducive to unstructured and structured data types that already exist within the organization. Since cloud BI solutions are often separate from the rest of the organization’s IT, there is risk for incompatibility with other enterprise applications.

**Costs Are Difficult To Quantify**

Cost benefit analyses for business intelligence are difficult, even more so with cloud solutions. Despite the presumed short-term cost savings and increased efficiency, “long-term savings from SAAS lie in reduced IT support costs and other factors,” [15] and are much more difficult to quantify without a control study. Gartner analyst James Richardson laments that returns on investment in cloud-based BI solutions have not been fully proven nor yet measured [21].
**Changing and Controversial Regulatory Environment**

Using the cloud to store and compute data complicates regulation, as there is increased likelihood of cross-border data storage and access. Brad Smith, General Counsel and Senior Vice President, Legal and Corporate Affairs at Microsoft, explained the implications of the Cloud Computing Advancement Act, legislation proposed to Congress by Microsoft to “build confidence for consumers and enterprises in the cloud,” [14]. The proposal asks Congress to modernize laws regarding the cloud to promote privacy and security. Other legal frameworks, like Stop Online Piracy Act (SOPA) and the Protect IP Act (PIPA, are highly controversial and also have the potential to affect cloud computing, security, and data regulation. Both BI vendors and users need to understand how government legislation affects them and act accordingly.

The industry is young, and the regulatory environment is changing. Currently, there is a lack of standards across independent vendors. As the industry matures, standards will rise and vendors and managers alike will learn important lessons. As a result, appropriate regulation will follow. Anyone involved in cloud-based BI should actively monitor and participate where possible in the legislative process surrounding the topic.

**PRECAUTIONARY REMARKS FOR CLOUD BI**

Prior to embarking on a cloud transition, the organization should utilize the concept of the “trusted computing platform.” This notion is similar to the value chain concept; the organization must establish long term relationships based on trust with the entities of the cloud. More specifically, all parties should be confident and assured that the cloud user is responsible for application-level security. It is imperative to the integrity of the organization that users within their cloud come from the trusted computing platform. In addition it must be mandated that all participants of the trusted computing platform implement a security mechanism on this platform to achieve the privacy and security individually. As a benefit to the organization, the cloud provider implements the physical security, in addition to enforcing external firewall policies. However the security for intermediate layers of the software stack is shared between the user and the operator.

As described, clouds are comprised of and configured with multiple entities. Among them are a great number of users with their own goals and behaviors. As with any pre-employment hire, or business partnership, due diligence should be conducted with all entities involved with the cloud relationship. In addition, different users have different security needs, so good design would offer a choice of security levels and security mechanisms. It is also recommended that those who use/access the organization’s information (data) should be classified into several classes or groups and access control criteria for each should be implemented. That being said, despite the classified access and no matter how robust the security system, the cloud is only as secure as its weakest link. It is the ethos of a cybercriminal to identify the vulnerabilities of an entity’s security system and to exploit it.

The lack of security associated with just one single entity within the cloud threatens the entire cloud in which it resides. If all participants of the cloud do not practice adequate security measures, it is almost certain the cloud will become a high-priority target for cybercriminals. More disturbing, and as determined by the inherent nature of the cloud’s architecture, clouds offer the opportunity for simultaneous attacks to numerous sites. As a result without proper security, hundreds of sites could be comprised through a single malicious activity.
In addition to operating on a trusted computing platform, Gartner Research [9] has identified seven cloud-computing security risks, which should be analyzed by an organization in an attempt to mitigate risks when embarking on the cloud. First and foremost, it is recommended that organizations get as much information as possible about the people who manage the organization’s data. It is also recommended that providers supply specific information on the hiring and oversight of privileged administrators, and the controls over their access. Organizations must be aware of cloud computing providers who refuse to undergo traditional external audits and security certifications, learn from providers if they will commit to storing and processing data in specific jurisdictions, and whether they will make a contractual commitment to obey local privacy requirements on behalf of their customers. Another important consideration is the attention to lost data and service in case of a disaster, as any offering that does not replicate the data and application infrastructure across multiple sites is vulnerable to a total failure.

Intel [7], [20] embarks on a high level cloud computing strategy taking advantage of SaaS for applications where there are clear benefits. However, they are very cautious about the type of applications suitable for external cloud. In fact, they use internal cloud for applications that:

- deliver competitive advantage
- are mission-critical
- are core business applications
- contain sensitive data
- are affected by network latency or bandwidth

CONCLUSION

Cloud computing promises significant benefits, but today there are security and several other barriers that prevent widespread enterprise adoption of an external cloud. In addition, the cost benefits for large enterprises have not yet been clearly demonstrated. A recent study [24] shows that 71% of the organizations consider Cloud Computing a realistic technological option, 70% believe that it would lead to increased business flexibility, 62% consider that it would speed up response to market conditions, and 65% consider that it would lead to increased focus on the main aspects of business.

Although the concept of the cloud is alluring to many organizations, the venture poses risks and vulnerabilities relating to organization’s data, personnel, reputation and existence. Some experts believe that threats to an organization’s viability increase exponentially with exposure in the cloud computing environment.

If after weighing the risks and rewards of embarking on the cloud, an organization deems it a worthy endeavor, it is imperative that the organization be diligent in mitigating the risks. As outlined in this paper this can be accomplished by operating on a trusted computing platform, conducting due diligence on the entities with whom the organization will be engaged, preparing for a disaster with an investigative protocol, and ensuring that data will be recoverable in the event the cloud “vaporizes.”
It would be further suggested that if an organization embark on cloud computing, that it initially be selective concerning the types of data it relinquishes to the cloud. That data which is deemed proprietary and relevant to the organization’s core competencies should remain in house. Just as an organization would not “outsource” its core competencies, nor should the organization “outsource” the information relative to its core competencies.

The impact of cloud computing to an organization’s bottom line could be extremely beneficial or detrimental, all of which is incumbent upon the preparation, planning and implementation of the process. It is hoped this paper provided some insight into the magnitude of the undertaking such an organizational decision will carry.

REFERENCES


