CHAPTER III

THREATS AND OPPORTUNITIES WITH CLOUD COMPUTING

INTRODUCTION

If and when the computer as we know it today may disappear, because:

- computing devices will integrate into other machines, and
- the IT culture itself will significantly change with the new generation of technologies.
- the current generation of technologists focuses on acquiring new machines rather than on increasing the cost-effectiveness of installed gear, and
- CIOs and their people pay little attention to the benefit from, and better management of, IT assets—adopting new technology only when and where ,h,,. is evidence of an excess of benefits over costs.

The new generation of information technologists, particularly those with a busi-ness education, is expected to behave differently.

Normally with software as a service platform bugs should not be on the radar screen, but they might show up unexpectedly as several onDemand providers devel-oped their routines without using virtual machines either because:

- they preceded the recent popularity of virtualization, or
- they did not have internally available virtual machine experts.

Software that gets out of the environment for which it was designed has the nasty habit of coming up with surprises. Even the change in the release of an OS brings up bugs the previous release did not flash out. Problems that filtered through the grid of platform A may come up with a vengeance when platform B is used or when the processing environment is too different, as in the case of*VM*. (In fact, the interpreter may be stumbling on the bug.

Hence, while we cannot be sure that the computer as we know it today will disappear, we should appreciate that several practices dating back to the 1950s and 1960s, like I/O bad policies

and Cobol, which are pillars of legacy IT, will fade. If they don't, the heralded flexibility and cost containment of cloud computing will take residence in the cuckoo cloud and not in the Internet cloud.

The CIO's Career Is at Stake

There are two types of threats associated with cloud computing. The one is pres-ent with all new technologies and can briefly be stated as missing the chance that might have been. Being afraid to find oneself at the bleeding edge is the typical error made by many when it comes to a decision about adopting a novel solution. Rush without adequate preparation is the other way to mess up things (more on this later).

There are many reasons why traditionalists are set to *miss their chance.* The most frequently heard excuse is that "senior management did not yet make a decision," which usually hides a mixture of fear and ignorance about what the new technol-ogy is all about. Other reasons for missing the boat include:

- lack of clear ideas on how to proceed,
- inadequate or incomplete preparation, and
- forcing the tool on the problem, which is itself ill-studied.

There is absolutely no reason to believe that all this will not be repeated with cloud computing. Subutilizing a novel technology is more or less a policy since day one of data processing. An example has been the ill-prepared transition to comput-ers from electrical accounting machines (EAMs).

Studies able to produce commendable results in transition to a new technologi-cal environment must cross department lines, but people who want to do a neat job are often told, "Don't touch the fiefs of colleagues." This ends up with mismanage-ment and with general deception in regard to corporate expectations.

More than in any other time it will be wrong to repeat with cloud computing these past practices because careers are at stake, and this does not allow spending time to preserve the status quo. The coming generation of information scientists, now out of universities, has a different culture than those who preceded it:

- the new graduates are Internet-minded, and
- because of the economic crisis, company management is bent not just to reduce head counts but also to have younger people at lower salaries at the service departments.

Since the beginning of this century, something senior management has brought directly under its watch is profitability and return on investment in IT. This means that without a significant change in concept regarding organization and end user services, a company can be sure of one thing: it will miss the benefits that could be derived from a strategic inflection point, whether or not it adopts cloud computing.

The financial advisability of cloud computing solutions is not at all self- evident. This is easily assessed from the uncertainty nowadays embedded in IT budgets.

Budgets are financial plans that, to be approved, require a lot of convincing evidence, and as of recently, they are tightly controlled. In addition, cloud computing essentially means outsourcing of services, and service level agreements (SLAs) often leave much to be desired. Closely associated with that is the risk of a lock-in by cloud vendors, as it has happened with mainframes and protocols.

Today the computer is no more the glamour instrument that it used to be. Data processing and telecommunica-tions have become services subject to ROI criteria like any other investment or expenditure.

This does not mean that the CIO must get everything about the cloud right from the start. What it means is that he or she should focus on the fundamental and be well informed in the study of opportunities, risks, and alternatives, which are nearly always around.

- “Me-tooism” is a sin, and this is also true of messing things up.
- By contrast, the careful study of competitive advantages and disadvantages is a virtue.

The obsolescence of human resources is nothing new with information technology. What is novel is that companies have at long last started to appreciate that they cannot afford any-more human obsolescence.

In addition, CIOs and IT departments must come to grips with the fact that not only individual skills and those of the organization as a whole wane, but also cloud computing may have unexpected consequences for which the company must have on-hand troubleshooters. For instance, the rising popularity of onDemand application may see to it that:

- a large part of the cutting-edge software talent from colleges and universities ends up working for cloud companies, and
- while user organizations will be reducing their head count, they will need some of the best graduates as troubleshooters working for their IT departments.

Providers must satisfy complex regulatory environments in order to deliver ser-vice to a global market. And if there is a major failure, the CIO's job will be on the block even if it was not his or her fault. In no time cloud hurdles may turn into a no-win/no-win situation.

Centralization May Be a Foe, Not a Friend

In IT, cloud computing may provide some of the ingredients necessary to ange concepts and applications, test new ideas, develop better procedures associ-ated with market opportunities, and serve customers in a way that involves people at all organizational levels. The bet on technology, however, should not be an asym-metric task favoring novelty but paying little attention to quality or failing to con-trol present and future costs.

Centralization of infrastructural and other services is a problem that both cloud computing vendors and user organizations have to confront—not "some time down the line" but now. A great deal in terms of quality results, and therefore marketability and profitability, will depend on how well service delivery coordinates and control at the vendor's side.

Managing change successfully begins with the ability to antici-pate the future, develop foresight about risks and opportunities, and sell change as a product. Integral to the management of change is the guts to measure devia-tions that result from incompetence or misjudgments—and take immediate cor-rective action.

Budgeting for Cloud Computing

A budget is a formal written statement of management's plans for the future, expressed in quantitative terms. The financial allocations^ the budget makes, and the statistics being derived from them, chart the course of future action. Provided that the budget contains sound, attainable objectives rather than mere wishful thinking, it serves as an excellent tool for planning and control.

- The budget is a *planning model*, and the means used for its development are planning instruments.
- *Budgetary control* works well when the company has proper methodology and solid cost data.

Fulfilling the premises of the second bullet will be rather difficult in the first years of cloud computing. The reason why a great deal of attention must be paid to costs is that the whole process of financial planning is based on them. Costing makes the budget an orderly presentation of projected activity for the next financial year,t based on the amount of work to be done.

In a well-run organization, management appreciates that planning premises entering a budgetary process must serve to increase its ability to rely on fact find-ing, lessening the role of hunches and intuition in running the enterprise. A factual and documented budget for cloud computing makes possible effective management control, including:

- a profit and loss evaluation vs. the current IT solution, based on information derived from the financial plan and operating'statistics, and
- other management controls that, among themselves, provide the standars against which actual performance is evaluated and variances monitored.

This needs to be done both for* each of the cloud computing services (onDemand software, platform(s), infrastructure, enabling) and for the project as a whole— hence in both a detailed and a consolidated way. An integrative view of accounts is necessary, starting at the system design level, translated into "bill of materials and services" and from there into budgetary premises.

Astute business executives have found out, some of them the hard way, that ROI in information technology is at its best when planning for it goes hand in hand with organizational change.

- organizational investments complement IT investments, each feeding on the return of the other, and
- ROI depends most significantly on a culture that promotes flexibility and adaptation to the system changes being introduced.

A valid budget for cloud computing will see to it that organizational change is costed and provided with funds. The same is true of educational expenditures that assist in cultural change.

- either the budget is incomplete, or
- nothing is done in reengineering and education, and therefore ROI will be a chimera,

The worst return on investment is obtained when companies are using IT purely as a way of doing "more cheaply" the same old things in the same old ways. That's why the argument that "cloud computing will cost less" does not wash. The best ROI is obtained when companies are able to take things apart and find new solu-tions, which is the role of reengineering:

- turning the organization inside out and
- rethinking the ' which the firm communicates internally and with its business partners.

Good governance requires that the budget be used as the basic tool for separating real output from the imaginary. This needs measurements and metrics, precisely the function to be played by a *budget analyzer,* which will track in an objective manner projections that have been made, authorized expenditures, and obtained results. This is of capital importance with outsourcing of services—and therefore with cloud computing.

Outsourcing, Infrastructural Interdependencies, and the Cloud

In a cloud computing contract, the user organization is the outsoucer and the cloud provider the insourcer. *Outsourcing* is the delegation to another party—the insourcer—of the authority for the provision of services. This is done under a con-tract that incorporates service level agreements

An SLA must be precise and include quantitative measures and qualitative descriptions of:

- functionality,
- cost,
- quality, and
- timeliness of services

Insourcing is acceptance for rendering specific services, under the above condi-tions. The insourcer is faced with the challenge of getting it right and the cost of getting it wrong. (Outsourcing and insourcing are not necessarily the best policy for every entity and every service, but this is not the present books subject.)1 Four main problems exist with outsourcing:

1. Cultural. Leading to agency costs (frictions and their aftereffects), as well as subutilization of resources and inordinate expenses.
2. Technical. Technology moves fast, and so does obsolescence in skills, soft-ware, hardware, and systems solutions. Constant updating is a steady chal-lenge with all technical issues.
3. Lack of proper methodology and conflicting methodologies. Because of het-erogeneity in systems, methods, tools, and languages, as well as backgrounds and line of authority of people assigned to the project.
4. Absence of quality criteria. These should be both quantitative and qualitative, as well as precise and measurable. Moreover, they should be contractually defined between outsourcer and insourcer, which is very rarely the case.

The pros say that outsourcing IT to a cloud provider has the potential to trans-fer management responsibilities to this party while at the same time reducing costs. This long-haired argument is total nonsense. Risks and responsibilities cannot be delegated by the outsourcer to the insourcer. Instead, both of them are confronted by major risks:

- strategic,
- reputational,

- contractual,
- operational,
- counterparty, and
- exit (more on this later).

Other exposures are country risk and compliance risk/ft All of them are present at the same time, because there exists a great lot of infrastructural interdependencies with cloud computing. Indeed, this infrastructural interdependence is critical in prac-tically all applications involving computers, databases, and telecommunications.

Outsourcing is not a relegation of responsibility. Most definitely, it is not a substitute to internal problem resolution. In fact, as in other areas of insourcing/outsourcing, the golden rule is

- don't outsource a problem you have, and
- if you have a problem, you fix it first.

The senior management of user organizations should appreciate that it is not possible to outsource its responsibility. The one-off discharge of management's duties and accountability has not yet been invented. Outsourcing is a situation where neither the supplier nor the customer is always right. Therefore,

- painful decisions have to be made, in terms of outsourcing IT services, and
- user organizations must appreciate that they cannot sign an outsourcing con-tract and walk away from it.

With cloud computing, too, while minor information outages may be common, meltdowns can be very expensive and highly risky—wiping out whole corpora-tions. This is one of the core problems with cloud computing. Reliability must be studied way ahead of any decision to outsource.

Other challenges come with multisourcing, which many user organizations consider the better strategy in connection to the cloud. True enough, companies that know how to put into effect a multivendor procurement have been reaping considerable benefits. But *multisourcing* is not a simple process, as it involves:

- avoidance of duplicating the development and maintenance process,
- challenges in effectively networking diverse computers and databases with diverse protocols and format,
- allocation and scheduling difficulties in resource sharing within the user's total system, and
- efficient operation in spite of differences in terms of support provided by mul-tiple vendors and associated contractual clauses.

There is as well the very important issue of *exit clauses*, which most often is not properly addressed, as if outsourcing always delivers as expected and the out- sourcer-insourcer partnership will last forever.

Theoretically the instability of outsourcing/insourcing pays into the hands of the biggest vendors. Practically, big companies, too, may not perform. From overly optimistic cost savings to poor deliverables, wanting quality of service, longer than contractual response times, and unacceptable cloud system reliability comes the day the outsourcing contract must end. If the SLA does not include detailed exit clauses, and if the user organization is not ready to take over for the insourcer, a multibillion disaster is the surest outcome.

Service Level Agreements

A service level agreement is a two-way contract that defines deliverables and their functionality, timing, quality, cost, and associated legal procedures. Because out-sourcing contracts can be tricky, it is always advisable to check their clauses with the user organization's lawyers prior to signing them. Legal issues should include guarantees in regard to:

- dependability of outsourced services;
- operational risk associated with these services;
- contract termination clauses and their reason;
- resolution of eventual conflicts, including conflicts of interest;
- penalties for noncompliance to contractual clauses; and

- the outsourcer's right to inspect facilities and staff of the insourcer.

The issues raised by the first four bullets have already been discussed. Let me explain why penalties for noncompliance are important, If penalties are nonexistent or are too low, *then* the insourcer may not care about whether or not it meets head-line service levels. Therefore, most definitely:

- SLAs should incorporate an escalation of penalties and
- lead to the option to exit the entire contract for severe or repeated failure.

In addition, as the last bullet in the list points out, user organizations should definitely retain the contractual right to audit the vendor's premises and practices. In case they buy infrastructural services, this becomes an absolute must. The aware-ness about auditing the insourcers, its premises, and practices has not yet come to life with cloud computing, yet:

- it is important in absolute terms, and
- it is a good way to reduce the likelihood of having to use the exit clauses.

The need for auditing cloud computing vendors and their premises is strength-ened by the fact that such outsourcing-insourcing associations between user and vendor are not expected to be ephemeral and should be looked upon as a partner-ship. Good accounts make good friends. A prerequisite to auditing a cloud vendor's services, however, is that the user organization is clear about what it expects to *gain* from outsourcing, answering by itself and to itself questions like:

- What do we want to reach through the vendor's cloud computing services?
- Which conditions will bring us from "here" to "there"?
- How do we keep the outsourcing-insourcing partnership in control?
- How do we develop and maintain contingency plans and exit strategies?

Cloud vendors should welcome these clarifications, because they oblige CEOs ai CIOs of user organizations to establish clear goals, evaluate risks and benefits from the cloud, review and document their existing operations, and set realistic expectations.

An integral part of a service level agreement for cloud computing must be the endor's assistance to the user organization, in case the latter wants to transit to a *private cloud.* Such an option is part of an approach known as *surge computing*, which retains the public cloud for providing the extra tasks that cannot be easily run in the private cloud of the user organization due to end-of-month heavy work-loads or other reasons. CIOs should nevertheless appreciate that surge computing:

- poses significant coordination problems and
- practically strengthens the probability of lock-in.

For all of the reasons presented in the preceding paragraphs, service level agree-ments should never be signed prior to examining the mistakes made in outcourcing by other user organizations and learning from them. Here is a short list of the most important I encountered in my experience:

1. Failure to focus on what exactly one needs to do in the short, medium, and longer term. For instance, which solution is cheaper *today* is important, but it only addresses part of the problem. The medium to longer term should also be part of a well-documented cost-benefit picture.
2. Decoupling cloud computing solutions from business strategy. Invariably,leaving aside the user organization's strategic goals or downplaying them
3. From overly optimistic cost savings to poor deliverables, wanting quality of service, longer than contractual response times, and unacceptable cloud system reliability comes the day the outsourcing contract must end. If the SLA does not include detailed exit clauses, and if the user organization is not ready to take over for the insourcer, a multibillion disaster is the surest outcome.

Overreliance by senior management on vendor promises. Examples are fail-ure to look at the insourcer's support policies with other user organizations, survivability, methodology, level of technology, human resources, and more. The result is badly chosen criteria for cloud provider choice.

4. Failing to test stated advantages, beyond cost savings, and to account for pitfalls. Pitfalls are not just a nuisance. They have associated with them delays, costs, and risks that are

important parts of the go/no-go picture. Failure to integrate them into a cloud decision is tantamount to going with the herd in outsourcing vital services. There is a snake pit of risks associated with such practices.

5. Little or no attention is paid to contract termination problems. The need for exit clauses has been discussed in Section 5.5. The shortfall resulting from their absence goes all the way from backup services to legal risk. Because the termination of SLAs for cloud computing is going to be a very painful exer-cise, I strongly recommend that the service level agreement also incorporate penalties for noncompliance, as has already been discussed.

The user organization should never give the cloud vendor, or any vendor for that matter, the feeling that the outsourcer-insourcer relationship is a blank check. This, for instance, happens when the vendor of cloud computing services, or its representatives, senses that the outsourcing organization is eager to transfer the *ownership* of a business process to the insourcer(s)—or that the user organization will consider the transfer of control.

Is Cloud Computing a Lock-In Worse than Mainframes?

Service level agreements should be explicit on both the threats and opportunities connected with cloud computing. One of the threats we have not spoken of so far is the risk that the cloud locks in the user organization to the vendors wares. It has happened over several decades with mainframes, and it is likely to happen again.

Indeed, there are legitimate reasons to worry about this possibility. Who will be the cloud service providers most successful in locking in clients tells a great deal about who is going to eat whom at the cloud level; that is, at the very top of the food chain.

Far from being theoretical, questions regarding lock-in deserve a great deal of attention. Critics compare policies followed with cloud computing to those with mainframes in the 1950s, 1960s, and 1970s. Overwhelmed by a storm of pro-prietary protocols, data formats, and languages, users had no freedom to install new applications on more cost-effective equipment provided by other vendors. Recompilation overhead and other expenditures:

- limited their freedom of action and
- increased in a significant way their costs.

One of the lock-in risks with cloud computing is connected to application pro-gramming interfaces (APIs). Because they have not been subjected to standardiza-tion, APIs for cloud computing are largely proprietary, with the result that user organizations cannot easily extract their programs and data in one process to run on another. This works to the user's disadvantage.

Anecdotal evidence suggests that concern about the difficulty of extracting information elements from one vendor's cloud to use in another's is preventing some organizations from adopting cloud computing. I think to this concern should be added another one, which is king size: policies urgently needed to deal with data decay on magnetic and optical supports.

During the last decade computer user organizations, which practically means all companies, have been confronted with the challenge to keep a step ahead of data decay, over and above the fact that their databases have been exploding. Since the late 1990s they have been creating new databases just to decipher information on mag tapes, mag disks, and optical disks. Together with government agencies, many companies looked into:

- durability tests and
- standards for digital media, which did not come on-stream as expected.

The problems connected to data decay are not limited to time and cost associ-ated with transcriptions. Information can be lost or corrupted as it is transferred periodically from one media or computer system to another. The better-managed companies have made *media preservation* a priority, when considering computer systems.

Some estimates bring the cost of managing online storage to over three hundred dollars per gigabyte per year, including tuning and backups. It needs no explaining that this is expensive, given that *petabyte* online memories are no more an undocu-mented hypothesis. The financial industry is leading the data storage explosion, but it is also the least likely to want to release its information elements to cloud providers because of:

- security,
- confidentiality, and
- probable legal cost reasons.

That's the case of what is called a double whammy: data decay problems mul-tiply while the required amount of storage capacity explodes. Efforts to increase longevity are not uncommon, but still, the better policy is regeneration and rereg-istration. This confronts the management of user organizations considering cloud computing with two questions:

1. Should the cloud provider be asked to fulfill that task? If yes, what sort of guarantees does the user organization have that it will not become massively dependent on the cloud computing vendor? Data lock-in is a different but deeper issue than being constrained by using applications and enabling ser-vices that the cloud provider offers.

In attempting to answer this query, the CEO and CIO of the user firm should factor in their equation that consumer lock-in is an attractive strat-egy to cloud computing providers—and specifically in the use of databases,, customers become vulnerable to price increases. In fact, the greater the lock-in of its customers, the more the cloud services vendor will be inclined to increase his price list through different gimmicks presented as quality or service upgrades.

2. What kind of assurance is provided by the cloud vendor that decay of stor-age media is confronted in a dependable and cost-effective manner? This query brings squarely into the picture the need for auditing of the vendor's premises, systems, and procedures, legally guaranteed by clauses in the SLA contract (Section 5.6). The quality and persistence of a solution providing assurance from data decay matter as much as the price to be paid, if not even more. Therefore, user organizations should not go for the lowest cost but also consider the degree of data dependability guarantees provided by the cloud vendor.