The Management of Risks within the Virtual Construction Project Environment

O. K. B. Barima
okbarima@yahoo.com
Dept. of Real Estate and Construction, University of Hong Kong, Pokfulam, Hong Kong

1.0 Introduction

Recent innovations in the information and communication technology (ICT) sector, have led to the emergence of the so-called concepts of the ‘virtual’ organizations and ‘virtual’ management in the construction industry and other economic sectors. Collaboration and lateral communication among geographically dispersed skilled individuals, firms and teams (e.g. environmental experts) is enabled through the medium of computer networking and other ICT tools, via the application of this management concept. With the view to achieving common goals, some of the characteristics of this model may be: teamwork, outsourcing, the maintenance of less physical presence, lateral communication and collaboration, reliance on modern ICT networking tools, and other dynamic factors. Teams may also be disbanded after the goals are achieved (Jarvenpaa and Liedner 1998; Oosthuizen, Koster and Rey 1998; Barima, 2001).

The ‘virtuality’ concept has both challenges and benefits, and the scenarios of failures and successes have characterized firms that ventured into this realm (Greenberg, 1999; Mandel et al, 2001). This brings to the fore the issue of opportunities and risks, and the need for strategies to minimize threats/risks and maximize opportunities/strengths; and more-so given the fact that construction projects are normally executed under relative uncertain atmosphere (e.g. uncertain weather conditions, etc).

This paper focuses on the discussions on risks of the concept of virtual construction project management, using the traditional risk management methodology of risk identification, assessment, mitigation and control.

The discussions will be done in this manner:

- First, the general framework of risks and its management processes are presented, and the various realms and interactions of a virtual construction project are identified.
- Secondly, risks are identified for an in-depth analysis and discussions, under the themes of: organizational, social or people issues risks, technological risks, communications security risks, legal risks and other risks, that may impact the ‘virtuality’ concept.
- Thirdly, risk assessment and evaluation is briefly presented.
Finally suggestions for risk response and mitigation for some of the identified virtual project risks are given. A brief case scenario to reinforce the need for the proper virtual construction project's risks management, to minimize risks and maximize strengths of the concept is finally presented.

2.0 The general framework of risk

Risks in systems can exist because one or more components in the system are risky, or it can result from components that are themselves relatively safe, but interact in ways that increase risks (Kerzner, 1984; Flanagan and Norman 1993).

The virtual management process can be seen as a system formed from the combination of various sub-systems of inputs, processes and outputs (the various virtual and physical components i.e. firms, information and communication technology [ICT], etc), which produce the whole final product. Each of the identified factors may have some risk exposure, or even if they are relatively safe, may have the capacity of interacting in various ways to make the whole virtual management process risky.

3.0 Risk management processes

Risk management could be said to comprise the following processes: risk identification; risk assessment (evaluation /quantification); solution development (maximizing opportunities and minimizing threats); risk control (continuous responsiveness), (Flanagan and Norman 1993; Oosthuizen, Koster & Rey, 1998). Risk management of the virtual process must involve all stakeholders on a continuous basis throughout the whole virtual project life-cycle (concept, development, implementation and close-out). The various ICT tools could assist in achieving this objective within the virtual project.

3.1 Risk Identification

Flanagan and Norman (1993) intimate that risks once identified and defined are no longer risky, but rather become a management issue. They however state that the poor identification of risks breeds further risk. Risks may be grouped as either controllable or uncontrollable (e.g. Acts of God etc). Controllable risks may be further sub-divided into issues within the control of others and those over which the particular firm has control (Flanagan and Norman, 1993). Risk identification therefore needs a comprehensive outlook, and virtual construction project risks may accordingly be grouped under controllable & uncontrollable issues for further attention.

3.2 Identification of risks within the virtual project environment

Two broad areas within which risks may be identified in the virtual construction project are: the virtual and the physical construction project components. The virtual risk component may comprise the information and communication world; the limitation on physical presence; outsourcing; and flexibility amongst others. The physical project risks will on the other hand, involve the actual physical design and construction activities that may be executed at the various phases of the construction life cycle.

Risks will however be identified for discussion under these themes: organizational risks; social or people issues risks; technological risks; communications security risks; legal risks; others.
3.2.1 Organizational risks

Risks could emanate from: within a specific firm; a firm to the virtual project interface; firm to non virtual project interface; virtual project to non project or other interfaces.

3.2.1.1 Within a specific firm

The following issues (among others) could lead to risks if found to be lacking within the virtual project process:

- Top management vision, quality of management and support for the particular virtual project; the potential ability of the specific firm to successfully handle similar projects; technological, personnel and equipment capacity; commitment of the firm to the works they handle; the firm’s integrity level and the management’s concern about it; and the general attitude of the firm to quality standards.
- The firm’s approach to change management (especially if it is the first time that the firm is dealing virtually) and any existing risk management systems which are employed by the firm; issues concerning resistance to change, for example, in adopting particular information and communication tools.
- The firm’s affordability of the access and maintenance costs into the virtual environment; lack of adequate ICT human resources, and the possible pitfalls of outsourcing; communications management position within the firm.

3.2.1.2 Firm to firm interfaces within the virtual environment

The following issues may need consideration:

- The equilibrium of divergent organizational cultures from the different interacting firms, which could potentially change traditional organizational characters.
- The stability of the push—pull effects between the alliances of workers for their parent organizations and that of the virtual entity, which could lead in some instances to loss of management control. For example:
  - how would a firm’s existing hierarchical communication orientation affect its workers working in an evolved horizontal communication culture or setting that may characterise the virtual process; and what would be the impacts of strategies like, say, telecommuting on firms.
- Risks associated with the administration or management of communication between firm to firm interfaces.
- A not well defined virtual project scope and objectives; the type of firms and project leader in charge of the virtual project (e.g adversarial with an affection for litigation, or a democratic leader).

3.2.1.2 Firm to non virtual project interface

One major question may be to ask: how will other current jobs being executed by firms affect the virtual project in terms of competition for resources (capital, technical and other resource flows) ?

3.2.2 Technology and communication security risks

3.2.2.0 Information and communication technology environment generally
The risks associated with the usage of ICT networking could be grouped under technological and communications security. Technological risks are firstly identified, before communication security risks.

3.2.2.1 Technological risks generally

Risks could be identified in some of these areas:

- The weaknesses of various firms’ ICT hardware (e.g. frequency of breakdowns, reliabilities and availability, compatibility etc); and other operational technological reliabilities within specific localities where participants operate from, to avoid for example: possible power black-out, or say complete communication blackout.
- The capabilities of the software applied at different places e.g. how often are bugs on browsers (which may allow easy holes for attacks or break-in) patched up.
- Computerized facilities risks may need specific identification and possible remedy, since this could form the back-bone of most virtual communications. Laudon and Laudon (1991) note that with data easily concentrated into electronic form, coupled with many invisible automated procedures requiring specialized skills, computer systems are vulnerable to destruction, misuse, fraud, data/information theft, and hardware failure; and the effects of a disaster in computerized systems can be much more extensive and in some cases, systems’ records can be destroyed and lost forever.

3.2.3 Communication security risks

The following issues as itemized below (sections: 3.2.3.1-3.2.3.5) may be identified under communication security risks.

3.2.3.1 Potential threat from many nodes

Since the information and communication internet/networking media can be accessed from many nodes within a network system, each of these nodes can be a potential threat (Laudon and Laudon, 1991). Example are vulnerability to hacking, worms, viruses and cracking etc. Moreover, congestion on the information superhighways may sometimes occur, and this may lead to the slow uploading and downloading of virtual project information.

3.2.3.2 Errors in database systems

In database systems, data can be used by more than one organizational unit and an error may reverberate throughout any particular reference network (firm). There may be less chances of detecting errors. Control may also be difficult as to the identification of who is misusing which information at any point in time (Laudon and Laudon, 1991).

3.2.3.3 Hackers, crackers, viruses, etc:

Arguably some of the most dreaded computer networking risks are concerned with the issue of hackers, crackers and viruses, worms and logic bombs.

- Hackers may hide worms etc in say a Trojan horse (a type of program) that can sometimes bypass security systems like firewalls etc. They may be sent as harmless pranks like obscene, political or love messages. These possess the potential to destroy data and even hardware (Dornan, 2001).
To be included under this section are the issues of the covert, overt and unintentional actions of employees that may lead to the loss of data, information, and damage to physical equipments (Elbert, 1992).

Microsoft’s case

A typical case scenario is the case of Microsoft company, a major player in the global computer market, which in the fall of year 2000 had its computer network hacked by a worm, which was apparently concealed within a Trojan horse. This resulted in the stealing of important company secrets in the process (Dorman, 2001).

3.2.3.4 Data transmission quality, privacy and authentication etc

Issues under this section may be on how to establish the reliability of the transfer of message, or data transmission quality, and prevent eavesdropping via the guaranteeing of the privacy of messages (Elbert, 1992).

3.2.3.5 Some problems with other communication connections apart from wire/cable

Though substantial networking connections may be by wired connections, the risks associated with other media (e.g. wireless/radio connections) will also need consideration, for example, the possibility of the interference and the jamming of wireless/radio applications; and the potential relatively expensive access costs for satellite communication.

3.2.4 Legal risks

The following issues identified below may give cause for concern.

- The legal environment of the information and communication networking environment is improperly defined, and countries are still in the process of evolving laws for this sector Johnson and Post, 1996; Department of Communication, South Africa, 1999).
- Because of the potential international outlook of the operation of the virtual project these possible issues may crop up:
  - conflicts of international laws; the ease with which one could enforce the rights, responsibilities and duties of the various parties operating from different geographic zones, even after judgments have been obtained (Hofman et al, 1999); and the general risk allocation mechanisms of any adopted contracts.
- Typical potential virtual project’s data risks in the course of a project. For example: in the case of the insolvency of the contracted information and communication service provider, what happens to the virtual project data?
- Conflicting legal issues, which the adoption of the virtual project may have with some existing well known traditional legal contract procedures. (For example, should the lines of flexible communications afforded by the virtual environment be introduced or encouraged, to allow the subcontractor to deal directly with the client or consultants, instead of through the main contractor, as most existing contract procedures encompass).
- Other potential legal challenges arising from the improper usage of the ICT networking technologies by the virtual project participants e.g. potential risks with digital signatures and other private confidential items if applied.

3.2.5 People/social issues
Though some of the identified issues under this section of ‘people/social issues’ could also generally apply to most traditional international projects, they are nevertheless worthy of mention. Specific issues which may be identified under the subject concerning people and other social issues are:

- Can trust evolve virtually? What are the pitfalls of trusting virtually?
- Cultural and language problems (especially if the project is of an international nature).
- Co-ordination and management problems within the different ‘time zones’ that project participants may find themselves in, e.g., the morning in say Japan may be the night and sleeping time in another country; and virtual project’s social impacts, associated with the lack of the maintenance of physical presence.
- Effect of the possible usage of different units of measurements, and technical presentations within specific different geographic settings.

3.2.6 Other project risks issues

The various traditional project risks like weather, inflation and others will apply for the physical construction sector of the virtual project.

3.3 Risk assessment/evaluation

This phase involves the determination of what risks to be dealt with, as well as how to set them into priorities. It will also include the assessment of the probability and impact on the project (Oosthuizen, Koster & Rey, 1998).

Risk analysis methods include the usage of both quantitative and qualitative analysis. The quantitative methods comprise: probability, scenario, simulation and correlation analysis. The qualitative analysis on the other hand includes the usage of direct judgment, ranking options, company options and descriptive analysis (Flanagan and Norman, 1993).

In the virtual project this will involve dealing with all the identified issues of risks. A checklist for the assessment of these levels of risks could be prepared to deal with the issues. Questions may include a re-look at: the crucial areas and levels of risks, the probability/ frequency of occurrence, the degree of seriousness and impact on the critical success factors of the virtual project etc.

A scenario
An impact assessment scenario involving a virtual project, which is being executed in South Africa, with designs being done collaboratively at different places in the country say: Johannesburg, Cape Town and Durban is illustrated below in Table 1. The relative potential possibilities of the occurrences of the listed events as indicated are all assumed. From the expected annual losses a decision could then be taken on which direction to take.

Table 1: A virtual project risk assessment

<table>
<thead>
<tr>
<th>Event expected</th>
<th>Probability</th>
<th>Assessed annual loss</th>
<th>Expected annual loss</th>
</tr>
</thead>
<tbody>
<tr>
<td>a) power failure</td>
<td>20%</td>
<td>1000000rands</td>
<td>20000rands</td>
</tr>
<tr>
<td>b) hacking *</td>
<td>1%</td>
<td>4000000rands</td>
<td>40000rands</td>
</tr>
<tr>
<td>c) programmes/</td>
<td>30%</td>
<td>20000000rands</td>
<td>6000000rands</td>
</tr>
</tbody>
</table>
* Impacts include: loss of access and its relative implications in terms of costs (labour; clean up and loss of machine time).

3.3 Solution development/risk response

Risks response to the identified and assessed risks may take any of the following forms: risk reduction, risk transfer, risk retention and risk avoidance (Flanagan and Norman, 1993).

Risk reduction involves the sharing of risks with others via education, training and the instigation of the behaviour (into people) to ask ‘what if’ questions and also alert them on potential risks in a consistent manner. Risk transfer removes the risks and gives it to a third party (e.g. insurance). Risk retention involves the retention of the risks by the party involved, whilst risks avoidance is synonymous with the refusal to accept risks (Flanagan and Norman 1993).

There may also be residual risks that are outside both the retained and transferred risks, which also need some consideration. The party that is in the better position to both control and manage the risks may be the best party to handle the risks (Flanagan and Norman 1993). Risk response may also include documented and determined alternative strategies including contingency planning, substitute plans in place for all ‘what if’ scenarios and insurance (Oosthuizen, Koster & Rey, 1998).

3.4 Risk mitigation suggestions for some of the identified virtual project issues:

The following are some risk mitigation suggestions to deal with some of the identified risks.

3.4.1 Organizational risks/ social & people issues:

- Proper change management practices must be adopted by firms to effectively deal with change from existing traditional concepts into ‘virtuality’, and its associated fallouts. Change could be managed as a project.
- Secure personnel with good project management skills and technical knowledge on: the risks of ‘virtuality’; the ability to draw in top management support; the setting of clear goals and objectives; good planning, team and trust building efforts (to form bridges across cultures, skills etc) and dealing with other conflict prone areas of the virtual project will be useful.
- Continuous training mechanisms through the application of the enabling ICT environment could be done in cycles to deal with any identifiable risks.
- On the probable high costs, lack of entry and adequate personnel, other cheaper service (reliable) providers may be assessed for outsourcing.
- Asynchronous and synchronous modes of transaction, together with team effort could be applied to solve the problems relating to time. Basic units of measurements could be agreed upon at the onset of the project, and plans clearly set out to deal with any deviations.

3.4.2 Technology/Information and communication networks issues:

- Adopt known, easily standardized, scalable reliable platforms (Elbert, 1992). Seek expert advice on these highly technical issues where necessary.
• Ensure adequate physical protective mechanisms (where necessary) against theft, abuse, lightning strike, water leakages (Elbert, 1992). If a buy/lease decision is taken, or in the case of hiring, enshrine this in the contract, and where possible always make power supply contingency plans to counteract effects of occasional power cuts e.g. generators, UPS (uninterrupted power supply), etc.

• Get proper networking administration in place (choose the right people for the right job). Conduct frequent networking security audits (Laudon and Laudon, 1991). Bring in trusted third parties where necessary e.g. software bugs in browsers etc must be investigated with a close watch via security companies to seal off possible holes for hackers. Get adequate security intrusion detection equipments in place, and install adequate security equipments (firewalls etc).

• Ensure consistent continuous education and training of users, on all possible potential networking risks, and warn against easy gullibility of users that could lead to infesting the system with worms, viruses etc.

• Conduct frequent data quality audits (Laudon and Laudon, 1991; Elbert, 1992); get regular data and other material backups and ensure adequate storage and security procedures for them (Elbert, 1992).

• Grade access to information stored on the network according to levels, giving the necessary access to information to people who are supposed or qualified to receive them (Laudon and Laudon, 1991; Elbert, 1992) and shield very important project information.

• In the case of hiring an application service provider (ASP), ensure that: the firm has the corporate strength, resources, commitment and relevant experience/track record to do the business to ensure acceptable quality and availability of facilities at all times; and also clarify in the contract how your data must be transferred to another (ASP), in case of the bankruptcy of the contracted service provider.

3.4.3 Legal

• Adopt project oriented contract documents that realistically distribute risks.

• Contract documents (especially international contracts) must clearly deal with all areas of possible conflicts. Issues could be on:
  ➢ which specific laws are to be applied; good conflict resolution methods; clearly defined responsibilities, rights, duties etc and how they would be applied; benchmarking some of the good existing contract procedures on: penalties and reward systems, payments, insolvency issues etc
  ➢ adopting clear litigation procedures to deal with issues of breach of trust. The better option, may however be to try to avoid litigation at the time of procurement/outsourcing the various participants by: ensuring that potential parties have the right track record; experience; resources; and good evidence of commitment to work etc. Partnering could be adopted where relevant. Guarantee (relative to the project’s value) the right quality and risk management plans/standards in place at the tender stage.

• Stress on the right type of performance bonds, payment guarantees and other securities, in the virtual project’s contract arrangements, to reduce risks.

3.4.5 Insurance

The virtual project could also take advantage of new electronic network insurance products or coverage, which have emerged. In this, insurance providers and security experts work together to improve the insured’s operating environment via a continuous cycle of identifying and eliminating risks. Insurance contracts are offered only after all
known risks are eliminated. A contract is then offered to diversify the remaining uncertainties (Yankee Group, 2000).

3.4.6 Contingency plans

Contingency plans must be developed for the worst-case scenarios, for example the scenario of a complete denial of service via hacking at the peak of the virtual project. Giving prior training to all the virtual project participants, so that what should be done at such times, will always be known at all times to them, will be a plausible idea.

There could be a constant backup of traditional communication mechanisms like courier services; physical face to face meetings; paper re-works; fax systems (in the case of the application of near perfect ‘virtuality’). Better still, applying some degrees of both the traditional and virtual concepts together could pay dividends.

In cases where computer-based communication networks are applied contingency plans like hot sites, warm and cold sites for contingency purposes could be adopted if available (Elbert, 1992).

4.0 ALERT CASE STUDY AND CONCLUSION

On the 15th of August, 1996 the CNN reported that, hackers successfully entered the United States of America’s (USA) Department of Justice’s official website and replaced text with pornographic pictures, President Clinton’s portrait with that of Hitler’s, and the background graphics with swastikas (CNN, 1996).

Analogous to a typical internationally scoped virtual project, this scenario could mean hackers successfully seizing a project website and then replacing the project’s information text with pornography, and all project’s digital pictures with that of sordid pictures at the peak of project activity.

Another scenario could be the denial of access to project information, or complete erasure of data, by the activities of hackers, in a typical virtual collaborative design. What will be the virtual project implications, if any of the listed events (e.g. complete erasure of data, by hackers) should happen in say: the designing for the critical construction of a failed bridge (that is the only link between two major economic cities) at a time when work is about 99% complete, and submission is due within the next 24 hours, in a contract that has time as the essence of the contract?

The implications in terms of claims and confusion could be many. Proper virtual project’s risk management is therefore very crucial and necessary, to avert the occurrence of any such disasters.

5.0 REFERENCES


ACKNOWLEDGEMENT: The author will like to express his gratitude to the G.E.Pearse Research foundation of the University of the Witwatersrand, Johannesburg, South Africa for supporting partly this research.