Journal of Computing and Information Technology - CIT 18, 2010, 2, 111–120
doi:10.2498/cit.1001816

Risk Effect on Offshore Systems Development Project Cost

Gerald DeHondt II and George Nezlek

Grand Valley State University, Allendale, Michigan, USA

Organizations frequently consider offshore systems development in the belief that projects can be completed at lower cost. While prices quoted by offshore vendors are often very appealing when compared with domestic vendors, additional risks must be considered when looking into offshore systems development. These risks typically take the form of intangible and indirect project costs which add to the total cost of the delivered system. This paper describes and classifies these risks, which fall into three primary categories of security risks, legal risks, and general risks. Suggestions for incorporating these intangible and indirect costs into the decision making process, and their effects on total project costs, are offered for the offshore v. domestic vendor selection process.

Keywords: offshore outsourcing, risk, systems development

1. Introduction

Organizations are under relentless pressure to reduce costs to preserve or improve their competitive positions. One of the most costly maintenance areas for many organizations is the Information Technology function (Barthelemy, 2001). An increasingly common choice for organizations seeking cost reductions is the utilization of third-party vendors outside domestic borders for systems development, commonly referred to as the "offshoring" of systems development. This alternative is based on the belief that a similar software product can be obtained from offshore vendors at a lower cost than developing the system in-house or with domestic vendors.

Costs associated with in-house and domestically outsourced systems development have been studied extensively in the literature. This paper develops a framework for considering the less understood indirect and intangible costs associated with offshoring systems development, and the effects of these expenditures on the total cost proposition to the client. In addition to direct costs paid to vendors, indirect costs - specifically for additional risks borne by clients when offshoring systems development - must be considered as part of the total cost of the system. Many bona fide risks and exposures associated with offshoring are ignored due to organizational exuberance about potential cost savings of global outsourcing (Goodman and Ramer, 2007). While explicit costs may be lower with offshore suppliers, the risks and implicit costs are lower with domestic vendors. When all of the costs and risk factors are taken into account, the net advantage of offshoring may be significantly and adversely affected (Shao and Smith David, 2007).

2. Literature Review

The relevant literature falls into three areas of interest. Discussions related to security issues, legal issues, and general financial issues are presented below.

2.1. Information Security

Using external vendors for systems development inevitably requires allowing external access to an organization's internal systems. Organizations can better control access to on-site information and facilities (McDougall, 2005).

Traditionally, external vendors may access software infrastructures, including the development, testing, and staging environments of the client. External access to organizational infrastructures potentially opens a backdoor through which hackers can enter, presenting risks that are nonexistent for internal development. It is incumbent upon organizations to maintain security standards, regardless of where development takes place. When multiple organizations are intimately linked, weaknesses in one can be used to attack another. Goodman and Ramer (2007) provide an example of a breach that occurred at Moneygram International, where corporate data were accessed through their business partner's site. Even though Moneygram was not at fault for the breach, their reputation was still negatively affected. Federal regulators warned: "You can outsource the function but not the accountability" (Goodman and Ramer, 2007). Exploitable weaknesses in offshore vendor systems can leave the client organization open to additional risks and their associated costs. Kark (2007) discovered that the average cost of a security breach is between $90 – $305 per lost record. As a specific example, Monster.com spent $80 million to upgrade their website after it was revealed that con artists had mined resume contact information from 1.3 million people (Hobson, 2008). Given these examples, it is incumbent upon organizations to realize the potential cost exposure when opening up proprietary systems to outside vendors, particularly if those vendors are based beyond domestic borders.

Another challenge in dealing with offshore vendors is a lack of standardized security procedures between industries and processes in different countries (Ramanujan and Jane, 2006). Managers considering offshoring systems development must ensure adequate security for offshored activities (Gonzalez et al., 2005).

Many organizations underestimate the difficulty of integrating offshore-supplier employees into their processes and workflows (Rottman and Lacity, 2006). The challenges include access to systems and corporate data, human resource issues, and the need to duplicate development and testing environments. These offshoring issues must be addressed prior to project launch.

2.2. Disaster Recovery

There are additional concerns with doing business in less developed or more volatile regions of the world. After the September 11, 2001 terrorist incident in the United States, many Indian offshore IT services companies created development centers outside of India for business continuity reasons (Chandrasekaran and Ensing, 2004). Recent political events and natural disasters have caused some business continuity concerns regarding Indian firms. These include the ongoing potential for a nuclear confrontation with Pakistan, earthquakes, and other natural catastrophes (King, 2005a). Organizations do not want critical development projects affected by natural catastrophes, Acts of God, or regional imbalances that may place strategic initiatives in jeopardy. Risks related to poor local communications and transportation infrastructures, common in India, sometimes require redundant backup offshore sites (e.g. the Philippines). In such scenarios, costs and risks associated with the redundant sites also need to be considered (King, 2005b).

Disaster recovery sites are often shared by multiple vendor organizations, and operate on a "first-come–first-served" basis. By using a single, shared backup site, multiple organizations face the risk of catastrophic failure when the 'eggs' of critical IT backup resources are placed in a limited number of 'baskets' (Snow et al., 2006). Given the proliferation of development vendor sites in countries such as India, it may be necessary for firms to operate multiple recovery sites as well, to geographically distribute or even fully replicate data and applications to prevent total loss (Twing, 2005).

Offshoring of IT services exacerbates system vulnerabilities by lengthening lines of communication and increasing the number of people, organizations, and computer networks that touch the data (Goodman and Ramer, 2007). Legal issues take on added dimensions and significance with offshore development. There are intellectual property and privacy concerns, which are discussed below.

2.3. Intellectual Property

Intellectual Property (IP) rights are often a gray area in developing nations, and organizations

experience increased risks of industrial espionage by competitors. For example, a former employee of an Indian outsource company allegedly offered trade secrets to a competitor after being fired (Fitzgerald, 2003). An ex-employee of an offshore vendor attempted to sell an IT company's proprietary information to a competitor because the country had no strong law enforcement mechanism to protect the company's rights. These cases reflect the types of additional risks borne by companies choosing offshore vendors. In a domestic relationship, these risks, and their associated costs, would be mitigated or eliminated.

Trade secrets may need explicit protection by contracts in an offshoring relationship. When offshoring, potential partners must safeguard confidential information against accidental, inadvertent or willful misappropriation, misuse, sabotage, loss or theft. If partners cannot be trusted to protect trade secrets, offshoring risks may far outweigh potential benefits. Hence, it is crucial to review the integrated security and IP protection program of any potential offshoring partner. Patent and trademark legalities have always been expensive and time consuming issues of an offshoring transaction (Pai and Basu, 2007).

The difficulty in defining legal protections for IP arises in the idea that some countries will favor local companies at the expense of foreign ones. To mitigate this risk, organizations need to assess a vendor country's track record on intellectual property protection, to verify the extent to which the business interests of all parties will be protected (Djavanshir, 2005). Client companies should also pay close attention to the experiences of other companies doing business in that country.

From a legal perspective, offshoring introduces other risks. When clients and vendors are headquartered in the same country, jurisdictional boundaries and parameters are clear. Across borders, the situation is less clear. In permanent work arrangements, employers are liable to third parties for employee negligence, and employees have a duty to protect trade secrets and confidential information (Arnett and Litecky, 1994). In the absence of an employment agreement, as may be the case with offshore workers, companies must take extra precautions to ensure that information is handled appropriately by contract workers. This may be accomplished through non-disclosure agreements, or other methods to ensure that proprietary information used by consultants is not disclosed to competitors.

Theft of intellectual property can occur without the knowledge of the affected company. Traditionally, software developed by a vendor for a particular client becomes the property of the client. Should the software company reuse the code for a different client, the original client may be unaware that their property is being resold. Legal systems in some countries may not be interested in or equipped to deal with these types of issues (Fitzgerald, 2003).

To address some of these risks, the World Trade Organization's TRIPS (Trade-related Aspects of Intellectual Property Rights) agreement attempts to standardize the protection of IP by member countries. However, this agreement is subject to local enforcement, and few popular offshore destinations have laws covering trade theft, although this is starting to change. For example, India, a popular offshoring locale, has drafted a patent law that is effective since 2005 (Ramanujan and Jane, 2006).

While popular offshore destinations are moving to address these issues, client companies must still invest time and effort performing due diligence of the countries in which they plan to operate, as well as reviewing the performance of the offshore vendors. Even with appropriate efforts, it is sobering to note that, according to the annual Business Software Alliance (BSA) Global Piracy Study for 2001, software piracy rates in India rose from 63 percent in 2000 to 70 percent in 2001 (Sengupta and Rajawat, 2002) and the estimated total of worldwide losses from software piracy has surpassed $50 billion (Business Software Alliance, 2009). Organizations may simply be unable to overcome the risk of operating in these types of environments.

2.4. Privacy

Different countries have very different laws relating to privacy and security. Many offshore engagements involve countries where privacy laws do not exist; or where there is much less,

if any, ability to enforce them if they did (Weinstein, 2004). This poses a significant risk to organizational data integrity and security of proprietary information (Murray and Crandall, 2006; Patterson, 2006; Ramanujan and Jane, 2006).

Offshoring lengthens the lines of communication and increases the number of people, organizations, and computer networks that touch the data (Goodman and Ramer, 2007). These additional connections with networks in multiple legal and political jurisdictions increase the risk of illicit access to information and pose considerable risks to the security and privacy of consumers' personal data. When business processes are offshored, so are the relevant sensitive data. Once the data are offshore, domestic protections no longer apply and many countries have far weaker security and privacy laws than the United States. For example, India has virtually no laws to protect personal and private data, and it is extremely difficult to use foreign courts to sue companies that misuse domestic data (Swartz, 2004).

Customers also bear the risk of privacy loss and identity theft with personal data entrusted to companies. For example, a Pakistani subcontract worker recently threatened to post U.S. patients' medical data on the Web if claimed back pay was not forthcoming (Weinstein, 2004). In these instances, companies must take proactive measures to control these risks, though it is unlikely that they can be completely eliminated (Patterson, 2006). In the specific case of offshored medical information, individuals have no rights under HIPAA to sue either U.S. companies that transfer data or the offshore companies that misuse those data (Swartz, 2004). Loopholes in the Gramm-Leach-Bliley Act also prevent U.S. consumers from suing banks if personal financial information transferred offshore is released (Swartz, 2004).

Employees of offshore vendors often have access to valuable and sensitive customer and transaction data, such as social security and credit card numbers (Ramanujan and Jane, 2006). Such information may be misused for corporate espionage, white-collar crime and terrorism. Companies must ensure that offshore centers are capable of maintaining appropriate safeguards for customer information and requiring them to implement and maintain such safeguards for client data. There are no enforceable international laws regarding data security, so offshore centers and U.S. companies need to jointly identify potential risks and work together to create an information protection framework (Ramanujan and Jane, 2006).

Reports of sensitive data being stolen or purchased from offshore service vendors increase concerns about offshore data security (Rottman and Lacity, 2006). This risk may be mitigated by distributing subsets of data among multiple vendors, so that the data become a puzzle that no one vendor can assemble on their own (Shao and Smith David, 2007). Risks to data privacy tend to be underestimated, with the possibility that employee data can be compromised at the offshore locations, resulting in identity theft. Organizations experiencing this type of data compromise face significant monetary loss or damage to their reputation (Shao and Smith David, 2007).

2.5. Political Risks

Offshoring means that a crucial organizational function is taking place in another part of the world. If this function is suddenly interrupted, the extra expense required to restart operations (either onshore or at another offshore location) can be considerable (Ramanujan and Jane, 2006). In a survey of senior IT managers, political risks, specifically relating to the political situation in a hosting country, are a major concern (Djavanshir, 2005). Offshoring exposes an organization to risks from political unrest and instability, wars, confiscations, nationalizations, and terrorism. These are in addition to the hosting country's governmental policies, regulations, and attitudes toward foreign businesses (Djavanshir, 2005). Any of these exposures considered individually, or as part of a whole, represents significant risk to the organization and potential financial exposure. In some developing countries, government rules and policies can change suddenly, and sometimes arbitrarily, based on individual decisions by heads of state. Political relationships between countries can also have a significant effect on business relationships, and can change significantly over time. Governmental action, expropriation, embargo or simply canceling licenses and permits for important businesses to operate can have a

considerable effect on business in that country (Ramanujan and Jane, 2006) and can cause client companies significant financial loss.

Political risk may also manifest itself in events over which an organization or its offshoring partners have no control - such as riots, political upheaval, new elections and war (Ramanujan and Jane, 2006). Other events may be caused by a government, such as an embargo on imports or exports, increases in tariffs, and new prohibitions on transactions with specific countries. Any of these could cause an interruption in service or even force the termination or abandonment of an offshore relationship leading to unintended expense. Businesses prefer to conduct offshore operations in politically stable countries (Davis et al., 2006). However, because wages coincidentally tend to be lower in countries that may be politically less stable, organizations looking only at explicit costs are often tempted to operate in such environments and unintentionally incur the requisite additional risk.

There are additional non-negligible risks of vendor compromise by organized crime or a hostile government to procure trade secrets or information to be used in financial crimes. Industrial espionage has often been supported by the intelligence services of foreign governments and the targets are often companies in nominally allied countries. In these situations, provider organizations and professionals are subject to forces beyond their control (Goodman and Ramer, 2007). In the specific case of India, although continued double-digit growth is expected in the offshoring market, there is a growing concern over political stability in the region (Jain, 2006). Even the policies of non-hostile allied governments cannot be taken for granted, as the disagreement between Apple and the French government over iTunes IP rights would suggest.

Aside from the challenges of doing business in other countries, organizations face political backlash and soured public relations at home when services and jobs are exported (Weiss and Azaran, 2007). In the United States, laws are being written to limit offshoring, and to encourage organizations to keep as much work within the country as possible. A majority of states have introduced legislation that would affect companies looking to offshore, or those already offshoring (Kukumanu and Portanova, 2006). For instance, New Jersey has banned offshore outsourcing of state government work (Pfannenstein and Tsai, 2004). Loss of consumer goodwill in response to offshoring efforts may end up costing companies well beyond any anticipated cost savings.

The preceding examples also suggest that many of the risks associated with offshoring may not neatly fall into easily distinguished categories. The final category of general risks this paper will address are financial in nature, and relate to international currency exchange.

2.6. Financial Risks

Currency values fluctuate, especially in less stable economies. Organizations must ensure that contracts with offshore vendors take the long-term effects of exchange rate fluctuations into account (Kumar and Eickhoff, 2006). Currency risks are a major concern, because changes in conversion rates might reduce earnings, and local inflation will directly affect a supplier's ability to operate. For example, firms operating in South America experienced the effects of runaway inflation in recent years (Kumar and Eickhoff, 2006). Firms dealing with European partners over the past decades have not only transitioned from local European currencies to the standardized Euro, but have also witnessed significant changes in the value of the Euro relative to the U.S. dollar.

In offshoring relationships, managing this type of currency risk can become a major issue. If the customer pays in a currency that falls in price relative to the vendor's currency, the vendor will experience a decreased profit margin. The opposite is also true - the customer must internalize the cost if the price of its currency experiences a relative increase. If this issue is considered in advance, the parties can address it in their contract through provisions that split the costs of exchange rate fluctuations between them. A periodic review, near the time a payment is due, allows for changing the fee to split the exchange rate difference between the parties (Weiss and Azaran, 2007).

2.7. Summary of Offshoring Risk Management Issues

Risk management is the process of proactively addressing environmental factors and events likely to affect a project. Despite the potential benefits of offshoring, it carries no more promise of success than in-house development or domestic outsourcing (Kleim, 2004), and in light of the additional risks incurred, may actually be a more doubtful endeavor. All projects involve some degree of risk. Some risks of offshored projects are identical to those faced by their non-offshored counterparts. Offshoring exposes firms to additional risks in host countries (Djavanshir, 2005), and the risks this paper considers are either unique to or exacerbated by offshoring.

It is important to note that many of the risks involving offshoring critical functions have not been fully recognized by firms engaged in such activity (King, 2007). Risk assessment and risk management need to play a larger role in vendor selection and in continuing relationship management. By identifying risks, and collecting and assessing information about them, organizations can incorporate accurate assumptions in their strategies and become increasingly proactive in mitigating and offsetting adverse outcomes. There are many ways in which an organization can manage these risks, but they all add costs to what is meant to be a cost saving venture (Fitzgerald, 2003). The cost of managing these risks potentially offsets the gains from offshoring in the long run (Kleim, 2004).

3. A Framework for Managing Offshoring Risks

Successful organizations continuously seek to improve operational and financial performance. Systems development is commonly viewed as a service area, and related costs are often the target of cost-reduction efforts. One popular cost reduction strategy is to transfer work to less developed regions of the globe, with an anticipated reduction in direct costs. This research studies the potential impact of risk associated with this strategy, as an indirect cost, on the total costs of systems development. By excluding indirect costs of risks unique to or exacerbated by offshore development, organizations do not consider the true total cost of offshoring.

The proposed framework categorizes the risks relevant to this discussion, and presents organizations considering offshore systems development with five propositions regarding offshored projects.

Proposition 1: Increased security risks inherent in offshore systems development increase overall project risk.

The United States places great importance on the protection of its national computing infrastructure. With the implementation of the National Infrastructure Protection Center (NIPC), now under the Department of Homeland Security, the federal government has in place an organization responsible for safeguarding the infrastructure networks and systems of the United States from attack. Many countries that are otherwise desirable offshoring locations simply do not have the resources, expertise, or possibly even the willingness to devote resources to these types of activities.

Additionally, the national infrastructures in less developed regions of the world are not of a level expected by domestic companies. Offshoring exposes organizations to risks of failures of governments and critical infrastructures such as power and telephone systems, and loss of faith of citizens in the ability of governments to function properly (Patterson, 2006). In situations involving natural disasters, public unrest, or war, foreign vendors may take longer to resume operations due to a weaker national infrastructure.

Proposition 2: Increased legal risks inherent in working with offshore partners increase overall project risk.

The United States has a strong legal system protecting intellectual property and individual privacy, and is viewed by the world as a stable government. Operating offshore places U.S. organizations outside U.S. jurisdiction, potentially leaving them less protected than they would be while operating domestically. Offshoring exposes companies to information vulnerability and security risks that can result from a lack of regulation and introduces new forms of risk by

creating more opportunities for incursion, accident, or exposure (Djavanshir, 2005; Goodman and Ramer, 2007). Many of these incidents are unlikely to be prosecuted or otherwise held accountable in many potential host countries.

Proposition 3: Increased risks inherent in offshore systems development add to the indirect costs of software development.

In offshoring systems development, companies believe that they will receive the expected software product, delivered in the expected timeframe, for a lower cost. The potential challenges and risks encountered when operating in less developed regions of the world are often excluded from the cost analysis. These include additional risks of security when opening up their infrastructure to business partners, increased risks of extraneous events or Acts of God affecting development cycles, legal systems that do not provide full protection to intellectual property and customer data, and risks from fluctuating currencies.

Taken together, these indirect costs can have unanticipated consequences and affect the overall cost to the organization. While risk can sometimes be shifted to other parties, there is little protection that can be afforded to an organization engaged in offshore systems development.

Proposition 4: Increased risk management costs inherent in offshore projects will increase overall project cost.

One of the key components of project management is the need to identify and control risks, which invariably adds to overall project cost. No project is ever completely devoid of such risks. Organizations must recognize that offshore projects will likely require even greater attention to risk management issues, due to the unique challenges in working beyond domestic borders (Kleim, 2004). Unfortunately, this is frequently overlooked when direct cost savings are emphasized as the justification for offshoring.

Proposition 5: Increased currency risk associated with offshore development will ultimately be borne by the client, increasing overall project costs.

Dealing with companies based in different countries raises the challenges of payments in different currencies. Regardless of which company will bear the consequences of currency fluctuations, the client will ultimately bear the risk. If the payments are to be made in the client's currency, this risk nominally shifts to the vendor. However, most vendors are financially smaller than their clients, and declining currency values and the attendant loss of purchasing power may significantly affect the ability of the vendor to continue operations (Gopal et al., 2003). Should an extreme situation occur where the vendor ceases operations, the client will be forced to locate a new vendor who can complete the project.

The relationship among the risk categories is shown in Figure 1. While the risks may fall into discrete categories, it is also possible that the specific risks an organization may be exposed to could span multiple categories. In such instances, and especially if resources are constrained, it may be of particular interest to identify the risk items with the broadest exposures as priorities, in order to maximize the cost effectiveness of risk mitigation efforts.

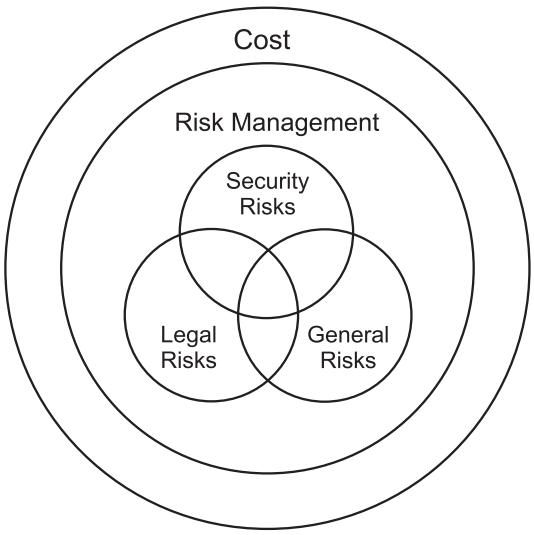

Figure 1. Risk factor summary and effect on project cost.

4. Discussion

It is all but tautology that systems development touches every area of an organization and enables an organization to produce a better product, or deliver better service, at the same or

lower cost. Since it is frequently viewed as a service center at many organizations, the systems development function is often the target of cost-reduction efforts. Despite the integral role played by systems development in organizational success, companies seek to have this function performed at the lowest possible cost, while paying scant attention to other significant systems related issues. Corollary arguments about diminished quality of systems are beyond the scope of this paper.

One of these additional risks is the security of information systems when working with vendors based in less developed countries. When partnering with offshore organizations, vendors will require access into the client's system, a potential backdoor vulnerability for the client and a valuable target for criminals. Considering that these criminals may be in other parts of the world, and effectively beyond prosecution, protecting these systems is now of utmost importance.

In a global computing environment, customers may access systems at any time of the day or night. This places additional emphasis on the need to have systems available 24 / 7 / 365. System downtime can have a significant financial impact. These factors require the ability of organizations to maintain system availability, and to quickly recover from any service interruptions.

With systems development occurring in less developed regions of the world, there is often less emphasis placed on intellectual property rights and individual privacy in some of these regions. As these systems are being developed, companies may also provide access to sensitive customer data to the vendor, placing the privacy of their customers at risk. Without appropriate safeguards, organizations may face significant financial risk from customer lawsuits or, at the very least, loss of customer goodwill.

There is also the question of how the vendor will be paid. Payments to the vendor in the domestic currency removes exchange rate risk from the client, yet may place undue hardship on the vendor in a period of falling currency values. Payments made in the vendor's home currency places the risk of currency fluctuations squarely on the client and may cause project costs to expand beyond original estimates. In either situation, the client bears the risk of fluctuating currency as they may be forced to pay the vendor in a weaker currency, or deal with a financially unstable vendor.

The additional risks inherent in performing systems development in less developed regions of the world are often overlooked, either inadvertently or deliberately, since the associated costs are often intangible and indirect, but may still be considerable. Offshore systems development projects are subject to the same inherent risks as domestic systems development projects, plus the additional risks, as previously described, which add to the overall cost to the organization. The contention of this paper is that traditional software development risks cannot be overcome but only managed, yet offshore systems development includes additional risks, and their requisite costs, which are not encountered in a domestic environment, but must be factored into the total cost of any project.

In the final analysis, offshore systems development places additional risks on an organization which may not be fully understood, and hence not properly mitigated. In certain circumstances, it is possible to shift this risk to other parties. In other circumstances it is not, and with offshore software development projects, the challenges are often greater. In many situations, it is simply impossible to transfer this risk to other parties, and the client company must ultimately bear the full burden of risk inherent in these projects, including the additional risks inherent in working with offshore vendors.

It is universally acknowledged that risk carries associated costs. In addition to the lower costs usually quoted by offshore vendors, the added costs of risk must be factored in. These indirect costs are seldom considered by companies at the outset of a project, yet may become painfully apparent once the project is under way. Ignorance is not bliss, and failure to account for the added risks of offshoring and their associated costs can have dire consequences for organizations that choose to see only the rosy picture of lower direct costs. This paper provides a framework to assist organizations in factoring in all of the costs of offshoring a systems development project.

5. Future Research

This paper presents a review of relevant literature and creates a preliminary framework, laying the foundation for future research in this domain. The propositions offered need to be translated into testable hypotheses, which defines the next stage in the authors' research agenda. In addition, the means by which to empirically validate the research model and test these hypotheses need to be formalized. Assessing risks in the context of finance and engineering projects is well documented, and many examples from the literature can be applied within the scope of this framework with little alteration. The authors foresee their greatest challenge in identifying organizations of sufficient scale or of similar characteristics to permit comparisons of offshored v. domestically outsourced development.

6. Conclusion

Organizations considering offshoring systems development need to be aware of the additional risks incurred by working beyond domestic borders. Systems development projects are risky enough in their own right, and working with partners that are potentially beyond reach introduces a number of other challenges that must be included in the final analysis. The challenge facing many organizations is lack of awareness of, or a deliberate decision to ignore these additional risks when considering offshore systems development. The increased risks of offshoring do have significant associated costs that need to be considered and included in the final cost calculation. This paper has provided a framework to summarize these risks and identified a series of issues for organizations to consider when offshoring is an option.

7. Acknowledgment

The authors wish to acknowledge the very helpful comments and suggestions of the reviewers of the initial version of this manuscript and participants at the 2009 Americas Conference on Information Systems (AMCIS). Incorporating their recommendations has resulted in a more ordered presentation and provided a better path for this research.

References

[1] K. ARNETT, C. LITECKY, Career Path Development for the Most Wanted Skills in the MIS Job Market. *Journal of Systems Management*, 45, 2, 6–10, 1994.

[2] J. BARTHELEMY, The Hidden Costs of IT Outsourcing. *MIT Sloan Management Review*, 42, 3, 60–69, 2001.

[3] BUSINESS SOFTWARE ALLIANCE, Sixth Annual BSA-IDC Global Software Piracy Study, 2009. (Available online at: `http://global.bsa.org/globalpiracy2008/studies/globalpiracy2008.pdf`).

[4] N. CHANDRASEKARAN, G. ENSING, ODC: A Global IT Services Delivery Model. *Communications of the ACM*, 47, 5, 47–49, 2004.

[5] G. DAVIS, P. EIN-DOR, W. KING, R. TORKZADEH, IT Offshoring: History, Prospects and Challenges. *Journal of the Association for Information Systems*, 7, 11, 770–795, 2006.

[6] G. DJAVANSHIR, Surveying the Risks and Benefits of IT Outsourcing. *IT Pro*, 32–37, 2005.

[7] M. FITZGERALD, At Risk Offshore. *CIO Magazine*, November 15, 2003. (Available online at: `http://www.cio.com/archive/111503/offshore.html`).

[8] R. GONZALEZ, J. GASCO, J. LLOPIS, Information Systems Offshore Outsourcing: A Descriptive Analysis. *Industrial Management & Data Systems*, 106, 9, 1233–1248, 2006.

[9] S. E. GOODMAN, R. RAMER, Identify and Mitigate the Risks of Global IT Outsourcing. *Journal of Global Information Technology Management*, 10, 4, 1–6, 2007.

[10] A. GOPAL, K. SIVARAMAKRISHNAN, M. KRISHNAN, T. MUKHOPADHYAY, Contracts in OffShore Software Development: An Empirical Analysis. *Management Science*, 49, 12, 1671–1683, 2003.

[11] D. HOBSON, The Real Cost of a Security Breach. *SC Magazine*, August 12, 2008. (Available online at: `http://www.scmagazineus.com/the-real-cost-of-a-security-breach/article/113717/`).

[12] P. JAIN, Offshore Outsourcing "India Vs China" An Empirical Investigation. *The Business Review*, Cambridge, 6, 2, 316–324, 2006.

[13] K. KARK, Calculating the Cost of a Security Breach. Forrester Research Report, Cambridge, MA, April 10, 2007.

[14] P. KAKUMANU, A. PORTANOVA, Outsourcing: Its Benefits, Drawbacks and Other Related Issues. *Journal of American Academy of Business*, 9, 2, 1–7, Cambridge, 2006.

[15] W. KING, Outsourcing Becomes More Complex. *Information Systems Management*, 22, 2, 89–90, 2005a.

[16] W. KING, Innovation in Responding to the "Threat" of IT Offshoring. *Information Systems Management*, 22, 4, 80–81, 2005b.

[17] W. KING, The IS Organization of the Future: Impacts of Global Sourcing. *Information Systems Management*, 24, 2, 121–127, 2007.

[18] R. KLEIM, Managing the Risks of Offshore IT Development Projects. *Information Systems Management*, 21, 3, 22–27, 2004.

[19] S. KUMAR, J. EICKHOFF, Outsourcing: When and how should it be done? *Information Knowledge Systems Management*, 5, 245–259. 2005/2006.

[20] P. MCDOUGALL, Northwestern Mutual Looks to Protect Customer Data Outsourced to India, April 5, 2005. (Available online at: `http://www.informationweek.com/news/management/outsourcing/showArticle.jhtml?articleID=160403815`).

[21] M. MURRAY, R. CRANDALL, IT Offshore Outsourcing Requires a Project Management Approach. *S. A. M. Advanced Management Journal*, 71, 1, 4–12, 2006.

[22] A. PAI, S. BASU, Offshore Technology Outsourcing: Overview of Management and Legal Issues. *Business Process Management Journal*, 13, 1, 21–46, 2007.

[23] D. PATTERSON, Offshoring: Finally Facts vs. Folklore. *Communications of the ACM*, 49, 2, 41–42, 2006.

[24] L. PFANNENSTEIN, R. TSAI, Offshore Outsourcing: Current and Future Trends on American IT Industry. *Information Systems Management*, 21, 4, 72–80, 2004.

[25] S. RAMANUJAN, S. JANE, A Legal Perspective on Outsourcing and Offshoring. *Journal of American Academy of Business*, 8, 2, 51–58, 2006.

[26] J. ROTTMAN, M. LACITY, Proven Practices for Effectively Offshoring IT Work. *MIT Sloan Management Review*, 47, 3, 56–63, 2006.

[27] S. SENGUPTA, Y. RAJAWAT, Copycats and Vanishing Income: Piracy is Rampant in India and China. Technology Companies Are Not Willing to Ignore This Anymore. *Economic Times*, August 8, 2002.

[28] B. SHAO, J. SMITH DAVID, The Impact of Offshore Outsourcing on IT Workers in Developed Countries. *Communications of the ACM*, 50, 2, 89–94, 2007.

[29] A. SNOW, D. STRAUB, R. BASKERVILLE, C. STUCKE, The Survivability Principle: IT-Enabled Dispersal of Organizational Capital. In *Enterprise Information Security and Assurance*, (M. Warkentin and R. B. Vaughn, Ed.), pp. 150–166. Idea Group Publishing, Hersey, PA USA, 2006.

[30] N. SWARTZ, Offshoring Privacy. *Information Management Journal*, 38, 5, 24–26, 2004.

[31] D. TWING, Could You or Your Outsourcer Handle a One-Two Disaster Punch? *Network World*, September 28, 2005. (Available online at: `http://www.networkworld.com/newsletters/asp/2005/0926out1.html`).

[32] L. WEINSTEIN, Outsourced and Out of Control. *Communications of the ACM*, 47, 2, 120, 2004.

[33] R. WEISS, A. AZARAN, Outward Bound: Considering the Business and Legal Implications of International Outsourcing. *Georgetown Journal of International Law*, 38, 3, 735–753, 2007.

Received: March, 2010
Accepted: April, 2010

Contact addresses:
Gerald DeHondt II
Grand Valley State University
Allendale, MI 49401, USA
e-mail: `dehondtg@gvsu.edu`

George Nezlek
Grand Valley State University
Allendale, MI 49401, USA
e-mail: `nezlekg@gvsu.edu`

GERALD DEHONDT is an Assistant Professor in the School of Computing and Information Systems at Grand Valley State University. Prior to his current role, he worked for Compuware Corporation providing consulting services to Fortune 500 companies. While at Compuware, he held increasingly responsible positions as a Programmer/Analyst, Quality Assurance Manager, Network Architect, Enterprise Architect, and most recently as a Project Manager guiding delivery of high-value projects.

Dr. DeHondt has taught courses at the Graduate and Undergraduate level in Information Systems Policy and Strategy, Project Management, Information Security, Management Information Systems, Systems Analysis and Design, Network Architecture, and Web Development. His research interests include offshore outsourcing of systems development and agile software development methodologies. He has a number of journal publications and his research has appeared at various national conferences, including the Decision Sciences Institute (DSI), the Americas Conference on Information Systems (AMCIS), the Conference on Information Systems Applied Research (CONISAR), and the Hawaii International Conference on System Sciences (HICSS).

GEORGE NEZLEK is Associate Professor and Information Systems Program Chairman in the School of Computing and Information Systems at Grand Valley State University. Prior to that, he held faculty appointments at Loyola University and DePaul University in Chicago, Illinois. While completing his PhD studies at University of Wisconsin-Milwaukee, he directed a private software and facilities management consulting practice.

Dr. Nezlek's research interests are in the areas of systems development methodologies, multi-platform computing, intelligent grid applications, and the applications of economic theory to problems in Information Systems. His research has appeared in leading journals and conference proceedings, including CACM and HICSS. His teaching experience covers a broad range of subjects, but his specializations are in databases and systems analysis. He currently serves as a vice-chairman of the Information Technology Interfaces conference and the EDSIG (ISECON/CONISAR) Board.