Acknowledging risks when deciding to outsource business processes: The case of "data theft"

Associate Professor Anne Rouse

Deakin Business School, Deakin University, Melbourne Australia

Email: anne.rouse@deakin.edu.au

Acknowledging risks when deciding to outsource business processes: The case of "data theft"

Outsourcing is generally framed in terms of benefits and cost savings, rather than risks. One important risk is "data theft". This paper draws upon a longitudinal study into IT and business process outsourcing to present a theoretical model incorporating risk. Sources include qualitative interviews with purchasers, non purchasers, and vendors of outsourced business process services. It concludes that data theft is an under-acknowledged risk in all business process outsourcing (BPO), but is higher for offshore outsourcing. This risk may be mitigated, but when factored into the business case can invalidate typically small cost savings. In acknowledging and adequately costing this risk, decision-makers may find BPO, particularly where offshore vendors are involved, less attractive.

Keywords: BPO, outsourcing, data theft, benefit/cost, business case

THE IMPORTANCE OF RISK IN OUTSOURCING DECISIONS

The last decade has seen the large-scale acceptance of outsourcing as a strategy, to the extent that now, businesses are exhorted to continually seek out opportunities for using outsourcing for all but "core" functions. Initially, reported outsourcing examples included relatively simple services such as cleaning, catering, or garbage collection, where it was argued outsourcing would lead to cost savings of 20 to 30 per cent accompanied by equal, or even better service quality (Domberger, 1986; 1987). Later, from the early 90s, firms have been encouraged to outsource substantially more complex services, particularly IT (information technology) services, again with the suggestion that this would lead to large savings (of 20 per cent or more), improved services, and redirection of corporate attention and resources back to core business (Lacity and Hirschheim, 1995). More recently still, firms have been encouraged to engage in "business process" outsourcing (BPO) often to offshore vendors, with similar levels of savings promised. Encouragements to outsource have come from many sources, including academic theory, but the major source of this advice has been vendors and consulting firms specialising in outsourcing (including the Big 4 firms and specialists like Shaw Pitman, the Metal Group and the Gartner Group).

Yet, for both simple services and IT services, empirical evidence of cost savings has been substantially less positive than the vendor-consulting promise. Hodge (2000), for example in his meta analysis of a range of outsourced government services, found that for simple services savings of between 6 and 12 per cent might be obtained, with an average saving of only 6%. For more complex services outcomes varied widely, and for those more difficult to define and measure, on average little or no savings were found and average cost savings estimates varied between an 8% saving to a 24% increase. Rouse and Corbitt (2003a) reported similar experiences for IT outsourcing in Australia, where only a minority reported cost savings, and a sizeable minority (22%) reported cost increases. Aubert et al reported similarly negative outcomes in their longitudinal Canadian study (1999) of IT outsourcing.

One reason for the failure of outsourcing to produce expected cost savings benefits is that the risks associated with the strategy are poorly understood. On one hand, the potential benefits of outsourcing, particularly cost savings and redirection of attention towards core competences, are widely promoted in the trade literature. Rouse (2006) confirmed that the extent to which expected benefits are achieved (particularly strategic benefits, technical service quality, and reduced costs compared to in-house delivery) predicts overall satisfaction with the outsourcing arrangement. On the other hand, she also identified that in more than half the cases (in a sample of 196) outsourcing purchasers' key expectations were **not** met, particularly their expectations for strategic benefits, and reduced costs. Outsourcing can also lead to a number of negative outcomes ─ including business inflexibility, service debasement, failure to protect confidential data or intellectual property (IP), and poorer

corporate performance. The extent to which either benefits are not achieved from outsourcing, or negative outcomes are consequences of outsourcing, represents the level of outsourcing risk.

Using the specific example of "data theft", a relatively serious, and it is argued, under-acknowledged risk, this paper illustrates that outsourcing needs to be understood in terms of benefits, costs, *and* risks, and that effective outsourcing management requires that the purchaser identify, and control all three elements. Risks are rarely highlighted by proponents of outsourcing, unless it is to suggest that they are easily managed by "good management practices", despite evidence to the contrary. While risks do not always invalidate the attractiveness of outsourcing, potential purchasers of BPO services still need to recognize the risks and take them into account when analysing the business case for adopting BPO.

Unfortunately, most strategic decisions are made on the basis of subjective risk, which are often quite at odds with objective and realistic risks. So when assessing the risk of outsourcing many decision makers appear to over-estimate the likelihood of benefits, and to under-estimate the likelihood of risks (Ang and Straub, 1998, Rouse & Corbitt, 2003a). An important role for academic researchers then is to obtain more reliable and objective data about the true likelihoods of both the risks and returns of outsourcing, so that the gap between subjective and objective (realistic) risk assessments is reduced. This should avoid the situations where overoptimistic subjective assessment lead firms to choose actions that, in the longer term, prove costly, or place them at greater strategic risk.

The paper draws on a six year program of study into IT and business process outsourcing in Australia. This study has included a large survey conducted in 2000, 12 focus groups covering 47 informants ,and 11 individual interviews with decision makers (CIOs, CEOs, outsourcing managers, and senior vendor staff). The purchaser firms were large Australian government and non government firms, generally in the BRW Top 100 listing, while vendors were large multinational vendors, some operating overseas (for full details, see Rouse, 2002). The paper first reviews the literature on outsourcing risk, then proposes a theoretical model for how risk affects the success of outsourcing. It then highlights a particular risk – that of "data theft" – and describes differences between the way this is treated by vendors, and the existing evidence. The paper concludes by recommending a number of actions firms can take to address this risk as part of the business-case on which business process outsourcing decision is made.

While definitions are fuzzy, BPO is generally described as the outsourcing of relatively complex business processes or functions that are supported by IT (information technology) and telecommunications networks (Halvey and Melby, 2000). It is the complexity, business impact, and the integral role of IT that distinguishes BPO from other, simpler forms of outsourcing. Examples include processing of back-end financial transactions (like the credit card transactions discussed above, or the preparation of tax returns), customer call centres, and sometimes functions like HR, customer billing, or even R&D. BPO is often described as being "not" IT outsourcing (and by implications, likely to be more successful) but in practice, IT outsourcing can also be seen as a particular form of BPO, that shares similar risks (Gewald and Franke, 2005).

THE IMPORTANCE OF DATA THEFT

Potential risks of outsourcing described in the literature include unexpected or hidden costs, service debasement, vendor default, vendor "lock in", theft of IP, and failure to adequately secure confidential information (Earl, 1996; Aubert et al, 1999; Wilcocks, Lacity and Kern, 1999; Aubert et al, 2002; Gewald and Franke, 2005). However, there has been a tendency in the literature to confuse causes (eg vendor or customer inexperience) with the actual risk (unexpected cost increases, service debasement, or loss of business flexibility). Gewald et al. (2006) classified risks into four categories: financial, performance, and strategic risks (which apply to the purchaser organization), and personal risks to the decision maker. In practice, performance and strategic risks are also financial risks, in that they will

have financial impacts. These authors included failure by the vendor to secure confidential data as one aspect of performance risk, however, the issue of data theft received relatively limited focus in their research, which involved the outsourcing by European banks to largely local vendors. In contrast, Australian research suggests that risks to data, particularly sensitive customer-related data that is the target of 'data theft', are a salient issue to potential purchasers and their customers, particularly when BPO involves "offshore" outsourcing (Rouse and Watson, 2005; McNair Ingenuity, 2006). Recent television and newspaper reports have highlighted substantial community concern that sensitive financial information, like credit card details, medical records, or taxation data, might fall into the wrong hands if it is moved beyond Australia's privacy protection laws through offshore outsourcing (7.30 Report, 2006; McNair Ingenuity, 2006). Such concerns have been magnified by the television broadcast last year (Four Corners, 2005) of an undercover newspaper investigation into the sale by a New Delhi vendor employee of 1000 UK customers' bank account details. Another influence would have been reports of the theft of sensitive credit card data for 40 million cardholders (including many Australians) from the US-based outsourcing vendor, CardSystems (Associated Press, 2005; Schumann, 2005). CardSystems is located in Atlanta, Georgia, where businesses are not legally required to notify customers of breaches to their sensitive data, and it was only as a result of an Australian investigation that this theft became public knowledge. As a result of this breach, Visa and American Express cancelled their contracts with CardSystems, but this action may have been taken too late to reassure potential and actual customers about the safety of their sensitive data.

The loss of critical records is, of course, not confined to outsourced vendors; USA Today (reported in Warmenhoven, 2006) has suggested that up to one in six financial records in the US were exposed to theft in 2005, many stolen directly from the data's owner. Thus data theft is a much more common risk than is generally perceived. However, the risks of data theft are magnified when highly sensitive personal information is passed to call centres or processing centres as part of a BPO arrangement (as were the Australian Visa, American Express and Mastercard records sent to CardSystems). This is particularly so when the destination is a country with poor data protection legislation (which, perhaps surprisingly, is the case for many US states).

The increase in "data theft" risk increases with outsourcing because data protection moves outside the direct control of the purchaser organisation. Outsourcing replaces the day-to-day supervision of staff, selected and vetted by a client firm with arms-length supervision of an external vendor through an outcomes-based contract. Theoretically, the penalties incorporated in the contract, the threat of contract cancellation, or the reputation effects that would accompany a major security breach, are sufficient to compel the vendor to properly manage the purchaser's sensitive information. In practice, as illustrated by the CardSystems experience, outsourcing controls like these do not always work, and they create the potential for dilution of responsibility. Contractual controls may be manageable for simple services (like catering or cleaning) where failure consequences have relatively low impact, but when it comes to more complex arrangements, especially where failure can result in widespread impacts, contractual controls appear limited. Furthermore, at this stage, because BPO is a relatively immature strategy, there is minimal empirical evidence on the outcomes of business process outsourcing (Gewald et al, 2006), so decision makers are required to accept on faith the capacity of contract-related controls to protect their organizational resources (such as sensitive data, or IP).

The emergence of internet-based communications and mechanisms for easily moving data between client and vendor databases were key drivers of BPO, and particularly offshore outsourcing, since such technologies overcome geographical distance. As a result of technical developments, western firms can now use lower cost labour from India or China (the major sources of offshore services for Australian businesses), or other developing countries, and so reap substantial salary savings. However, it is not always recognized that BPO services can only be supplied by lower-cost offshore vendors if the client hands over its sensitive data to the vendor in digital form. This digital data is relatively easily accessed (and copied) by the vendor's front-line operators, who may have limited loyalty to the company. Because of the centrality of sensitive data to the business processes involved, BPO has significantly higher risks than does the delegation offshore of factory-based manufacturing.

There the risks of losing key data and intellectual property (IP) are mitigated by the fact that front-line staff rarely have easy access to them. Manufacturing IP is far more likely to be held as tacit knowledge within the purchaser organisation, or in the form of blueprints and schematics that are easier to protect.

There is a ready market for stolen identifying data (commonly labelled "identify theft"). The data can enable unauthorized purchases; access to the victim's finances; illegal immigration; and even framing the victim for a crime (Wikipedia, 2006). These would have disastrous consequences for individuals, and helps explain the high level of community concern about this aspect of offshore outsourcing. Identify theft will also have substantial repercussions for the purchaser firms whose customer (or citizen) data has been stolen. These repercussions are of two kinds: the first is the potential for legal sanctions, given that in Europe, Australia, and increasingly the US, firms are subject to legislative privacy requirements which apply even where outsourced services are employed. Such sanctions might be from customer law suits, or from legal obligations imposed on firms and their officers by legislation. The second, and probably more important repercussion, is the effect publicized thefts have on firms' reputation and brand, and their customers' willingness to trust them in future. This loss may even drive the company into bankruptcy, or in the case of public sector agencies, cause substantial political damage. This was illustrated recently, where several senior executives of the US Department of Veterans Affairs were forced to resign after the theft of millions of veteran's names, birthdates, and social security records (Lee, 2006).

A MODEL OF OUTSOURCING RISK AND RETURNS

The risk of data theft can be understood from the point of view of two bodies of theory: *transaction cost economics* (TCE) and *risk management theory* (eg Crouly et al, 2001). TCE considers the strategic "make or buy" decision in terms of the interplay of production and transaction costs. Outsourcing vendors promote the economic argument that competition in the marketplace generally leads to lower production costs compared with in-house delivery (through economies of scale and scope, and through experience curves). However, there is less mention of the other focus of this theory, that is, the higher costs of dealing with the marketplace. Transaction cost economics highlights that these "transaction costs" ─ the costs of finding, contracting with, and controlling the work of the vendor, and of protecting against opportunistic behaviour ─ are sometimes so high that it is cheaper in the long run to keep the services in-house (Williamson, 1985)

Another cost that has to be balanced against production cost savings, is the cost associated with risks – particularly reputation and litigation risks. A risk is a *possibility* of "loss", this may be an undesirable outcome (the company receiving public opprobrium) or the failure to reap an expected outcome (e.g. expected cost savings, or redirection of attention to core business). Some risks involve negative outcomes (like large-scale customer defection, or legal sanctions) that may be relatively unlikely, but very costly. Research into managerial decision making reveals that managers tend to discount low-probability extreme events, and so their true costs (Bernstein, 1996).

Risk management theory suggests that risks should be quantified in terms of the magnitude of likely "loss" multiplied by the probability. This is the calculated "risk exposure", which is a potential, or notional cost of an action. In relation to "data theft", even though data breaches from outsourced vendors may be relatively rare, the magnitude of their impact means their risk exposure can be high. Risks with high levels of risk exposure can substantially impact the projected benefit/cost analysis that should precede any outsourcing arrangement.

Growing emphasis on governance and accountability now demands that these risks be better articulated, monitored, and managed. The US Sarbanes-Oxley Act, the US Health Insurance Portability and Accountability legislation, and European and Australian privacy legislation, have increased the risk exposure to purchasers by increasing the "loss" associated with poor controls over

data (Rouse and Watson, 2005). These forms of legislation place far greater personal and legal obligations on Board members, and CFOs, which are not reduced when processes are outsourced to external organizations. As an example, Section 404 of the Sarbanes Oxley Act requires that internal control procedures be in place to protect against "acquisition, use, or disposition of the assets that could have a material effect on the financial statements" (George and Gaut, 2006 p 24). Firms must require outsourced service providers to have documented financial processes, formal risk assessments, and adequate controls in place, and confirm that these controls are thoroughly tested for effectiveness. This responsibility cannot be devolved to the service provider. CEOs and CFOs are now personally accountable for the accuracy of financial data provided to the US SEC and the public, with the possibility of imprisonment if the information is not accurate. This legislation is having effects beyond the US, and substantially raises the importance of safeguarding corporate data.

The need for decision makers to trade off potential cost savings against transaction and risk costs is illustrated in Figure 1. Unfortunately, production cost savings are relatively obvious (and if they are not, the vendor will make them clear) while transaction costs are less clear (Ang and Straub, 1998). The potential costs associated with risks, are even more difficult to identify and quantify. While risk exposure is usually reported in dollar terms, another important risk exposure for outsourcing is the managerial attention that outsourced arrangements require if problems are encountered. In their research into IT outsourcing Rouse and Corbitt established that only a minority of purchasers reported that outsourcing allowed them to redirect attention back to core business (Rouse and Corbitt, 2003a), suggesting that this form of risk exposure is much higher than recognized. This is the exact opposite of the scenario presented to potential purchasers by vendors and consultants, and illustrates the importance of using evidence-bases to determine risk exposure.

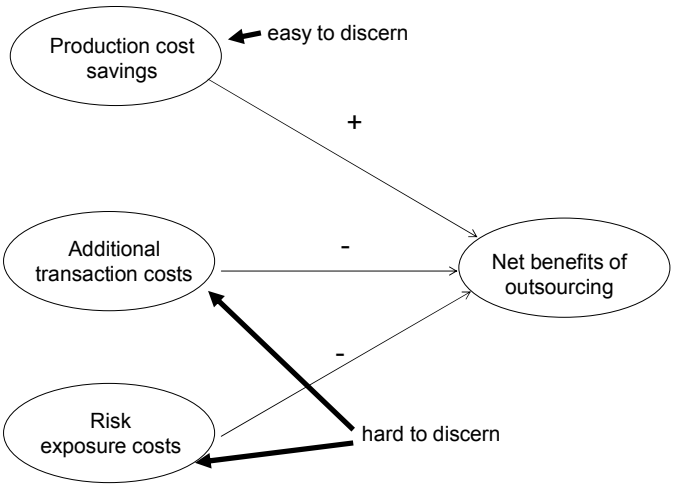

Figure 1: Costs saved from outsourcing depend on the relative balance of production, transaction, and risk costs

FINDINGS

According to several of our informants who investigated, and rejected outsourcing, when risks are identified and their impacts carefully costed, the financial arguments for outsourcing (particularly offshore outsourcing) are substantially less compelling. Like Ang and Straub (1998) who established that supporters of outsourcing tended to discount transaction costs while opponents tended to

emphasise these, we noticed that where purchaser decision makers rejected outsourcing, they seemed more aware of the risks associated with outsourcing (both on and offshore).

We also observed that both transaction costs and risk exposure costs were downplayed in the organizations keen to outsource their business processes. Few seemed aware of the newly-raised impacts of data theft brought about by privacy and other legislation.

Several of the outsourcing purchasers we interviewed found that their services had been moved offshore, sometimes without their knowledge, in an attempt by vendors to protect their dwindling profit margins. Other purchasers were not able to tell us whether this was the case or not – they simply didn't know if their contracts protected against this, or if their vendor (or its subcontractors) was using offshore labour.

One vendor informant told us (in 2004) that there were strong pressures on call centres to move from relatively expensive Asian countries (eg Singapore, India) to substantially cheaper countries (China, the Philippines, Vietnam) because of growing skills shortages and consequent rise in the price of labour. He argued that such moves introduced new challenges (and expenses) to vendor firms, because of the relative lack of training and infrastructure in these "even lower-cost" offshore markets. Another vendor informant drew our attention to the fact that most non-European offshore vendor markets (including many US states) lacked enforceable laws to protect company's intellectual property.

A vendor informant suggested that when offshore labour is used, an additional risk dimension is added, because contracts entered into may not be practically enforceable in foreign jurisdictions. One way this can occur is if legislative sanctions are absent. According to George and Gaut (2006) no data privacy protection legislation exists in India, the most frequent source of offshore labour for Australian BPO contracts. These authors report that, for example, the Indian Information Technology Act enabled in 2000 did not specifically provide for protection of sensitive personal information, and amendments proposed by the Indian Ministry of IT in 2004 had not yet been enacted at the end of 2005. In the absence of effective privacy legislation, and the threat of personal impact (such as jail), while it may be possible to legally sue vendors for failing to meet contract provisions, the lack of sanctions means this possibility may not act as an effective deterrent.

Furthermore, as one of our vendor informants told us, even if legislative sanctions are in place in offshore locations, a legal contract only acts as a form of control if it is enforceable, and the real power of a contract lies in the legal systems, and the audits and verification (backed up by the threat of punitive damages and of customer backlash) in which the contract is embedded. These in turn require vigilance on the part of the purchaser, and a culture in which theft and corruption are seen as socially deviant. Thus a second source of increased data theft risk is marked differences in cultural attitudes to privacy and corrupt behaviour (including data theft).

George and Gaut (2006, p. 3) argue that "despite the growing convergence of international data protection policy, "privacy" means something very different in various cultural and national traditions" and several of our informants noted that attitudes to corruption, and to the role of the contract, differ markedly across cultures. One informant drew our attention to Transparency International's "Corruption Perception Index" , where, in 2004, China was ranked only 71st; India was ranked 90th; and the Philippines and Vietnam ranked 102nd. By way of comparison, Australia has a rank of 9 (very low in corruption), while the US was ranked 17 (Transparency International, 2004). Hence while major vendors may be perceived by purchasers as having high levels of trustworthiness, these vendors may not necessarily be able to enforce behavioural controls on their staff in high-corruption countries. Our discussions with purchasers suggested that many outsourcing clients do not think seriously about the issues of cultural attitudes to privacy or corrupt behaviour because they are so embedded in their own national culture, where legal protections are taken for granted. (In contrast,

those who had considered, but rejected, outsourcing did consider these risks). Managers from countries with well established and corruption-free legal systems (like Australia and New Zealand, Singapore, and the UK) do not necessarily recognize that a contract entered into in countries where corruption is far more prevalent may have little practical effect on the behaviour of staff, even if it is technically enforceable. Although vendors may claim (as did one quoted in the Four Corners report) that "I can assure every Australian customer and consumer… that in a comparative sense at least [India] is among the safest places" such assurances are relatively meaningless. Where there is no legislation compelling firms to advise customers of theft of their personal records (the case in Asia and many US states) it is not really possible to get an accurate picture of relative "safety", and our informants suggested that the lack of legal and social infrastructure in many offshore destinations can mean that, in practice, the security of sensitive records may be compromised.

Purchasers (and rejecters) of BPO services amongst our informants also revealed that if outsourcing arrangements "go wrong" a new set of unforseen costs occur, as the purchaser must either bring back the services in-house (something that in many cases is impractical due to the start-up costs and timeframe), or move the arrangement to another vendor (also costly). Several of our informants reported that their organisations continued with quite unsatisfactory outsourcing arrangements because they could not afford the financial costs, distraction to managerial attention, or organizational disruption associated with changing their supplier.

DISCUSSION AND IMPLICATIONS

Overall, our research has shown that many managers do not appreciate the risks and downsides of outsourcing. They do not recognize that there are substantial uncertainties associated with promised benefits materializing (like cost savings and redirection of firm resources and attention), nor do they realize the size of the losses (including legislative and customer-perception related) that they may encounter. Consequently, our findings echo those of Hirschheim (interviewed in Healey, 2002)) who based on his extensive research into outsourcing argued that much decision-making associated with outsourcing is based on "wishful thinking".

Rouse and Corbitt (2003b) identified that a key determinant of outsourcing success is the accuracy of the benefit-cost analysis associated with the business case for outsourcing. They also demonstrated that even with expert advice from international specialist firms, the business cases for many of the Federal Government's IT outsourcing arrangements were fundamentally flawed. Effective decision making requires that the human propensity to downplay remote risks (like the theft of customer data) be recognized, and that the business case include a substantial analysis of the risk exposure involved. Ideally this would be based on independent, empirical evidence, where that existed, and a detailed exploration of usually-untested assumptions (e.g. that the probability of large-scale data theft is "low", when suggestions are that, even in the US, such theft is frequent).

Table 1 provides a checklist of questions decision makers should ask themselves about the likelihood of data theft. Answers should inform the benefit/cost analysis, and be compared with an assessment of the likelihood of benefits accruing. In many cases estimates of risks will come down to personal "guesstimates", so decision makers should make allowances for their enthusiasm to outsource their business processes. The more enthusiastic decision makers are, the more cautious should be these estimates, to avoid the "confirmation bias" that decision makers are known to be subject to (Kahneman et al., 1982).

While this probabilistic approach is used regularly in complex project management, it does not appear to have been used in many large-scale outsourcing arrangements, where the probability of achieving expected benefits is implicitly assumed to be 100%. Yet, empirical, independent research has demonstrated that the benefits of outsourcing are themselves subject to significant risks – expected cost savings are frequently not achieved, claims of increased quality from outsourced vendors have

not been substantiated, and the management of outsourcing has been shown to absorb significantly more managerial attention and resources than expected (Rouse and Corbitt, 2003b).

Given the error margins around "likely benefits", the tendency of enthusiastic purchasers to discount transaction costs, and the potential losses associated with data theft, it is possible that the benefit/cost/risk equation no longer adds up after critical scrutiny. If outsourcing is still attractive after answering the questions in Table 1, the additional thinking and planning associated with outsourced business processes will not have been wasted. Careful analysis is likely to lead to greater clarity when dealing with the vendor, and in the long term, greater levels of cooperation and trust. Such analysis will also assist firms meet their growing obligations in relation to legislative demands.

A GENERAL APPROACH TO MANAGING OUTSOURCING RISK

Table 1 addresses only the specific issue of data theft, which, while an important risk, particularly for offshore outsourcing, is only one of the many risks associated with the strategy. To address these risks, purchasers need to introduce a systematic and comprehensive risk management process as part of their sourcing decision-making. This involves, first, analysing the likelihood (probability) of losses – not easy when a number of forces discourage the publication of information related to failures. Not all risks are equally hazardous, so the second step is to establish the likely impact of the risks to the purchaser, so as to identify those that are most costly, or critical to purchaser performance or stability. It is important to examine unquestioned assumptions when this is done. Recent legislative changes, and the high level of offshore outsourcing have substantially altered the relative impact of data-related risks, so what has, till now, been perceived as a relatively low risk has risen in importance.

Having identified important risks, and gauged their potential impact, purchasers need then to institute measures to mitigate them. In relation to data theft, purchasers should investigate the privacy and intellectual property laws that apply to the vendor (and any subcontractors), and importantly, their realistic chances of enforcement. They should also ensure that their contract requires data protection procedures on the part of vendors (such as encrypting data at multiple levels, and banning the use of mobile phones and flash drives). For those risks that are not easily mitigated, decision-makers need to build into the business case additional contingency costs and think carefully about whether the risk should be borne at all. Since the capacity to control some outsourcing risks is often quite limited, and the contingency costs associated with identified risks can be very high, detailed risk analysis process often ends up making the original business case for outsourcing far less attractive..

Identified risks need to be controlled, that is, the strategies in place to mitigate the risks need to be implemented and tested, using the approach of "trust, but verify". Contractual provisions that are not audited and reinforced have limited effect on behaviour. Using the example of data theft discussed in this paper, purchasers should contract for unannounced, independent, third-party inspections of security behaviours. Purchasers should also demonstrate that they are serious about security issues. A final important, aspect of outsourcing risk management is to recognize that by outsourcing business services, firms cannot devolve their own risks – ultimately the purchaser still remains responsible in the eyes both of regulators and of customers.

Table 1: Questions purchaser firms should ask in relation to data theft risks

Legal obligation risks	Customer/reputation/brand risks
What are your firm's legal obligations if confidential data is released or stolen? What personal obligations do officers have?	On the basis of past experience how likely is it that your outsourced data or intellectual property will NOT be subject to data theft? (This should be based not on vendor assurances but evidence)?
Have you required your vendor to ensure multi-level encryption of sensitive customer data to prevent access by employees? Is this audited on an ongoing, and unannounced basis?	How are your customers likely to react if they discover their sensitive data has been released/stolen?
What legislative sanctions, other than contract provisions, are in place to ensure the behaviour of your vendor, and the individuals working for it?(e.g. privacy obligations that involve substantial personal fines and/or jail)	What will the long-term repercussions be to your reputation, brand, and customer trust if this happens?
What independent audit/accreditation has been required in your outsourcing contract? (The independent agent should be paid for, and report to the purchaser, not the vendor).	Has an allowance for the cost of recovering customer trust been included in the benefit/cost calculations?
What is the level of corruption in the country your vendor operates in? (Higher levels mean less reliance can be placed on legal sanctions)	Has an allowance for the cost of moving to another vendor (or re-insourcing the function) if the vendor proves unsatisfactory been included in the benefit/cost calculations?
Are customers in a position to sue your firm if you do not adequately protect their sensitive data?	
What insurance does your vendor have to cover liabilities that might arise from potential law suits against your own firm?	

In summary, our research has revealed many successful outsourcing arrangements, with satisfied purchasers and vendors. However, we have also seen outsourcing business cases that are over-optimistic, and that have not made adequate financial provisions for risks which are predictable. This leads to "surprising" cost blow outs, and is responsible for much of the dissatisfaction we observed in our quantitative studies.

The contingencies that allow organizations short term flexibility and protection from risks are real aspects of the benefit/cost analysis on which the outsourcing business case depends, and need to be budgeted for. If that means the business argument for outsourcing becomes much weaker, this is an important warning that should be heeded. BPO presents challenging problems - with new legislative demands, the involvement of offshore parties and a customer base alerted by recent data failures - and the management of BPO arrangements is becoming a mission-critical activity. Paying attention to the downsides, having realistic, evidence-based expectations, and planning for risks like that of "data theft' makes good business sense.

REFERENCES

7.30 Report. (2006). *Business 'offshoring' gains momentum – broadcast June 20, 2006 on ABC's 7.30 Report*. Transcript available from www.abc.net.

Ang S., & Straub, D. W. (1998). Production and transaction economies and IS outsourcing: A study of the US banking industry. *MIS Quarterly, 22*(4), 535-552.

Associated Press (2005). Visa, Amex cuts ties with CardSystems: Payment processor left 40 million accounts vulnerable to hackers. *Associated Press Release, July 19, 2005*. <www.msnbc.msn.com> [12 June, 2006].

Bernstein, P. (1996). *Against the Gods: The Remarkable Story of Risk*. Wiley, NY, NY.

Crouhy, M., Galai, D. & Mark, R. (2001). *Risk Management.* McGraw Hill. NY. NY.

Schumann, E. (2005). Data theft case proves need for new disclosure law. *Ziff Davis CIO Insight*. July 22 2005. available from < www.cioinsight.com> [12 June, 2006]/

Domberger, S., Meadowcroft, S.A. and Thompson, D.J. (1986) Competitive Tendering and Efficiency: The Case of Refuse Collection, *Fiscal Studies*, 7(4), Nov, pp 69-87.

Domberger, S., Meadowcroft, S. and Thompson, D. (1987) The Impact of Competitive Tendering on the Costs of Hospital Domestic Services, *Fiscal Studies* , 8 (4), pp 39-54.

Kahneman, D., Slovic, P., & Tversky, A. (1982). *Judgment under uncertainty: Heuristics and biases.* Chichester: NY: Cambridge University Press.

McNair Ingenuity Research (2006). Attitudes to Offshore Labor: *Report Prepared for Services Unions of Australia*. May 2006. [Available from the Authors]

Earl, M. (1996). The Risks of Outsourcing IT, *Sloan Management Review*, (Spring), pp. 26-32.

Aubert, B. A.; M. Patry and S. Rivard; (1998). Assessing the Risk of IT Outsourcing, *Proceedings of the 31st Hawaii International Conference on System Sciences*.

Aubert, B. A.; S. Dussault; M. Patry and S. Rivard; (1`999). Managing the Risk of IT Outsourcing, *Proceedings of the 32nd Hawaii International Conference on System Sciences*.

Aubert, B., Patry, M., & Rivard, S. (1999). L'impartation des services informatique au Canada: Une comparaison 1993-1997 (Outsourcing of IT services in Canada: A Comparison 1993 - 1997). M. Poitevin (Ed), *Impartition: Fondements et analyses (Outsourcing: Foundations and Analyses)* (pp. 202-220). Montreal: Canada: University of Laval Press.

Gewald, H. and J. Franke; (2005). A Comparison of the Risks in Information Technology Outsourcing and Business Process Outsourcing, *11th Americas Conference on Information Systems*, Omaha, NE, USA, 2005.

Gewald, H., Wullenweber, K., and Weitzel, T. (2006). The influence of perceived risk on banking managers' intention to outsource business processes: A study of the German banking and finance industry. *Journal of e-Commerce Research*. 7(2). 78-96.

Willcocks, L., Lacity M., and Kern, T. (1999). Risk Mitigation in IT outsourcing strategy revisited: Longitudinal case research at LISA, *Journal of Strategic Information Systems*, 8 (3), pp. 285-314.

Four Corners (2005). *Broadcast of the ABC's Four Corners program "Your Money and Your Life" 15 August 2005*. Transcript available from www.abc.net.

George and Gaut, 2006 Offshore Outsourcing to India by U.S. and E.U. Companies: Legal and Cross-Cultural Issues that Affect Data Privacy Regulation in Business Process Outsourcing. *UC Davis Business Law Journal*. 6(2). http://blj.ucdavis.edu/ [22 June, 2006]

Halvey, John K. & Melby, Barbara M. (2000) *Business process outsourcing: Process, strategies, and* contracts NY:Wiley.

Healey, C. (2002). Sourcing Strategies, *MIS* 11(2). 34-41.

Hodge, G. A. (2000). *Privatization: An international review of performance.* Boulder, Colorado: Westview Press.

Lacity, M. C., & Hirschheim, R. (1995). *Beyond the information systems outsourcing bandwagon: The insourcing response.* NY: Wiley.

Lee, C. (2006). Theft of data leads to firings: Moves at VA. *Washington Post*. May 31, 2006, p A17.

Rouse, A. C. (2006). "Explaining I.T. Outsourcing Purchasers' Dissatisfaction". *Proceedings of 10th Pacific Asia Conference on Information Systems (PACIS),* Kuala Lumpur, Malaysia. July 7 10

Rouse, A. C. (2002). *Information technology outsourcing revisited: Success factors and risks*. Unpublished PhD Thesis. University of Melbourne.

Rouse, A. C. and Corbitt, B. J. (2003a). Revisiting IT outsourcing risks: Analysis of a survey of Australia's Top 1000 organizations, *14th Australasian Conference on Information Systems 2003, delivering IT and e-Business value in networked environments*, pp. 1-11, School of Management Information Systems, Edith Cowan University, Perth, Western Australia

Rouse, A. C. and Corbitt, B. J. (2003b). The Australian Government's Abandoned Infrastructure Outsourcing Program: What can be Learned?, *Australian Journal of Information Systems,* Vol 10, No 2, pp. 81-90.

Rouse, A. C and Watson, D. J. (2005). Cyberfraud and Identity Theft. *Monash Business Review* 1(2). 30-33.

Transparency International (2004). *Corruption Perceptions Index 2004*. www.transparency.org/cpi/2004 [11 November, 2005]

Warmenhoven, D. (2006). Protect me, protect my data. *Business Week Online*. June 8 2006. <www.businesweek.com.> [12 June, 2006]

Wikipedia, (2006). *Data Theft*. http://en.wikipedia.org/wiki/Data_theft [12 June, 2006]

Williamson, O. E. (1985). *The Economic Institutions of Capitalism*, Free Press, NY, NY.