

Reining in Outsourcing Risk

For further information:

Jeffrey Tucker, New York: jeffrey.tucker@booz.com

Eduardo Alvarez, Chicago: eduardo.alvarez@booz.com

Jens Niebuhr, Düsseldorf: jens.niebuhr@booz.com

Booz & Company

11/30/2005

strategy+business (www.strategy-business.com) and Knowledge@Wharton (<http://knowledge.wharton.upenn.edu>) publish white papers on contemporary global business issues, featuring the latest research and ideas from partners at Booz & Company and faculty from the University of Pennsylvania's Wharton School. *strategy+business* is a quarterly business thought-leadership magazine published by Booz Allen Hamilton. Knowledge@Wharton is an online resource for executives published biweekly by the Wharton School.

Reining in Outsourcing Risk

Exporting business processes raises the potential for trouble, but companies can do much to reduce the threats.

As business process outsourcing (BPO) has taken off in recent years, so have concerns over the risks that come with it — everything from isolated instances of identity theft to large-scale disasters that could seriously disrupt operations. Corporations and their customers are extremely sensitive to data security breaches — so much so that a solitary incident could unleash a ruinous chain reaction, like the one experienced by third-party payment processor CardSystems Solutions in 2005. In June, an estimated 40 million credit and debit card numbers were stolen from CardSystems' Tucson offices. As a result, Visa and American Express canceled their contracts with the company, and MasterCard insisted on new security guidelines. CardSystems CEO John Perry told a congressional committee investigating the incident that the company “is being driven out of business” by departing customers. Finally, in October,

CardSystems was acquired by Pay By Touch, a San Francisco-based provider of biometric authentication and payment systems.

This incident is only one in a rash of security breaches at third-party contractors in 2005:

- In February, ChoicePoint, a major provider of identification- and credential-verification services based in Alpharetta, Ga., sold the personal data of some 145,000 individuals to criminals posing as small firms. The company later said it would “discontinue the sale of information products that contain sensitive consumer data, including Social Security and driver's license numbers, except where there is a specific consumer-driven transaction or benefit” or a law enforcement purpose.

- In April, several employees at BPO firm mPhasis in Bangalore, India, were caught using client passwords to fraudulently withdraw funds from the New York accounts of Citibank customers.

- In June, an employee at BPO

firm Infinity e-Systems in New Delhi sold the account numbers and passwords of 1,000 bank customers to a reporter from the British tabloid *The Sun* for \$5,000. (The names of the breached banks were not disclosed.)

- And most recently, on November 12, four former employees of Indian call center operator Parsec Technologies were arrested for allegedly stealing classified information. Parsec services housing mortgage originators in the U.S., and the ex-employees had diverted the contact information of potential mortgage finance customers to a firm they had set up called Telequest Systems, which in turn passed the information on to other call centers. The scandal came to light when there was a sudden drop in the productivity of call centers hired by Parsec.

Paul Fielding, program director at Booz Allen Hamilton in Dallas whose specialty is international outsourcing and offshore relationships with financial institutions globally,

says the risks are nothing new. The moment work goes “outside your four walls,” he notes, the potential for risk rises: “Once you do a transaction and open yourself to the Internet, the ether of that Internet flows around the whole globe.” Jon Watts, a principal with Booz Allen in New York City who specializes in technology strategy, notes that one of the reasons outsourcing carries such a high degree of risk is that “the companies themselves are one layer removed from being able to control the transparency of what is happening.”

Fearing loss of control, outsourcers have begun asking their service providers to incorporate tighter checks and balances in their work processes to secure data privacy and prevent fraud, say experts at Booz Allen and the University of Pennsylvania’s Wharton School, as well as others who closely track the BPO sphere. BPO clients are making it a priority to transplant their “best practices” to their outsourcing service providers, complete with documentation requirements and periodic audits. In addition, some companies are employing new tracking systems that enable them to monitor their BPO assignments

sure is also mounting on governments in BPO destinations like India to tighten privacy and intellectual property laws, and also to step up law enforcement.

Three Types of Risks

Apart from plain old thievery, the outsourcing industry faces three broad types of risks, says Ravi Aron, Wharton professor of operations and information management and a leading authority on outsourcing trends:

1) Operational risks show up as slippages on time, cost, and quality. Professor Aron says these frequently arise with breakdowns in the transfer of work processes, or in repetitive processes that are prone to human error. He notes that operational risks don’t arise from deliberate misbehavior; instead, they’re most likely to occur when the service provider does not completely understand a client’s requirements.

2) Strategic risks are rooted in deliberate, opportunistic behavior by service providers or their employees. Theft of intellectual property is the most common — but far from the only — example. Another type of strategic risk involves providers who cut corners by understaffing. A

switch suppliers.”

3) Composite risks manifest themselves when a client company has outsourced a process for so long that it can no longer implement the process for itself, says Professor Aron. “For instance, over a period of eight to 10 years, a retail financial-services company may not have any back-office operational capabilities if all of its retail customers are managed by offshore contractors in Mauritius or Manila,” he says. That could present problems when the client company has a new product and discovers that an entire set of needed in-house skills has eroded. Professor Aron adds that such risks have a relatively easy solution: Companies can retain minimal residual capacities so that they always have in-house access to outsourced skills.

Operational and strategic risks call for multipronged preventive measures. The first step, says Paul Fielding, is for client companies to recognize that “when you outsource a task, you don’t outsource the responsibility and accountability for that task.” For example, the client company can better manage data privacy by making sure no individual has complete access to the information. “In a financial institution, it is important to break up responsibility so that no one person can put the organization at risk,” Mr. Fielding says. To achieve that, he says, companies must understand the workflow and the supply chain to identify points of risk and then put in place preventive valves. The cases he has tracked all involved a single point of failure, and thus “they could all have been prevented.”

Mr. Fielding also cautions against overreliance on hardware and software as security blankets.

The moment work goes “outside your four walls,” the potential for risk rises.

in real time. BPO providers, meanwhile, are performing more stringent background checks on employees and, in the case of some larger BPO firms, are instituting zero-tolerance policies for security violations and underperformance. Pres-

third is what Professor Aron calls an “asymmetry of dependence”: “All goes well for three years, and when the contract comes up for renewal, the contractor doubles the price because he knows the client is locked in and it is not easy for it to

More firewalls don't necessarily mean increased security, unless they are appropriately administered, he says, adding that many companies have become lax on best practices. Even so, companies must ensure that their technology stays current, including virus updates. "For every piece of [security] technology, there is somebody out there thinking of a way to beat it," he says.

Focus on the Weakest Link

Outsourcing companies should also focus on interdependencies, says Howard Kunreuther, Wharton professor of business and public policy and an expert on risk management and insurance. "The challenge in

ty professor Geoffrey Heal. He offers the example of an apartment owner who tries to protect himself with smoke detectors, alarms, sprinklers, and other measures. An insurer would not be impressed, unless all the neighbors in that apartment building have taken similar protective measures. "This issue of interdependency is completely untapped and is probably the most important issue to start thinking about with regard to risk," says Professor Kunreuther.

Security problems are interdependent when risk faced by one firm is determined in part by the behavior of others, says Professor Kunreuther. More important, the

sengers who initiate the trip with that airline are inspected; those bags transferred from another airline are not." So it is with interdependent computer networks: They note that "once a hacker or virus reaches one computer on a network, the remaining computers can more easily be contaminated." The potential uncontrolled exposure in this scenario reduces the incentive for an individual computer operator to protect against outside hackers. "Even stringent cybersecurity may not be particularly helpful if a hacker has already entered the network through a 'weak link,'" they write.

U.S. financial-services companies have already bought into the need for industry-wide action. Identifying and managing outsourcing risk is an ongoing theme at BITS (once known as the Banking Industry Technology Secretariat) in Washington, D.C., a nonprofit consortium of 98 banks and financial-services institutions. Over the past two years, a 40-member IT service-providers working group at BITS has produced four documents to serve as guides for member organizations as they devise their risk management strategies. "These documents are comprehensive and provide recommendations and considerations throughout the entire outsourcing life cycle," says Faith Boettger, a senior consultant at both BITS and at the Santa Fe Group consulting firm in New Mexico who helped to develop them. "The

Outsourcers have begun asking their service providers to incorporate tighter checks and balances to secure data privacy and prevent fraud.

supply chains and outsourcing is, how do you begin to get a better handle on managing risk when you have interconnects among the various groups," he says. "One weak link in the system can bring all of the others down." Professor Kunreuther draws cues from work he is currently doing on inspections and quality control with Wharton professors Serguei Netessine and Stanley Baiman and Columbia Universi-

behavior of the other firms affects the incentives of the first firm to reduce its exposure to the risk. Professor Kunreuther studied this challenge in a paper on airline security he cowrote in October 2002 with Professor Heal and Peter Orszag, a senior fellow at the Brookings Institution in Washington, D.C. "Even an airline with an infallible screening system is at risk," they write, "since only the bags checked by pas-

report is written from the financial institution's perspective as a user: What are financial institutions required to do, what controls can be put in place commensurate with the risk, and what background information may be available by country."

The BITS offerings include everything from a survey of the key considerations in background screening of employees to recommendations on termination clauses in outsourcing contracts. But even the BITS work can't cover every eventuality. There isn't always a right answer for an institution weighing a certain type of risk, says Ms. Boettger. Much depends on the nuances and the risks inherent in the service outsourced. "We have provided considerations organizations can use to manage risk, not measure risk," she cautions.

Extend the Organization

Many risks can be avoided if outsourcing companies successfully transport their best practices to service providers, says Booz Allen's Paul Fielding. Doing that is far more than a matter of words on paper; rather, clients and providers need to work closely together on an ongoing basis. "Ofentimes, what I see in contracts is people trying to abdicate their responsibility with contractual language, and often the vendors are left in charge of checking themselves," says Mr. Fielding. The guiding principle, he says, is

"trust, but verify."

But how? Wharton's Professor Aron advocates an "extended organization form," a model that brings together two forms of governance — one imposed by the outsourcing "market" and the other by the in-house management, or "hierarchy." "The chief discipline of the 'market' is efficiency of cost, while the 'hierarchy' brings managerial control,"

clients to monitor a project's progress online, exercise quality control, and track the performance of small teams and even individuals in real time. Office Tiger's TigerTracks works similarly. Both tools track four or five times the number of performance metrics that clients request — a significant feature, according to Professor Aron. "One of the reasons they are able to do it is because of the

Client companies can better manage data privacy by making sure no individual has complete access to information.

he says. "The extended organization form will give a company the great benefit of contracting with a third party provider for cost control, and also the ability for real-time control of that project's performance."

The key to the extended organization is a so-called program office, where the client company and the outsourcing provider collaborate with the help of a finely calibrated monitoring system. He cites two companies that are successfully implementing that concept: IT services provider Wipro of Bangalore, India, and Office Tiger, a BPO firm based in New York City with its main outsourcing operations in Chennai, India. Wipro uses Velocity-Q, a proprietary system that allows

belief that they should become an extension of the client organization," says Professor Aron. Jon Watts, of Booz Allen, pushes the notion even further: "It's got to get to the point where the outsourced provider and the client company may form alliances and take financial stakes in one another to make sure their interests are aligned."

Security concerns, Mr. Watts argues, are a brand-perception issue for the BPO industry — one that threatens growth. In a recent Booz Allen Hamilton survey of offshore security, 24 of the 30 respondents perceived a high risk of threats to their companies' systems and data at offshore outsourcing locations. Mr. Watts suggests that the industry

could model itself on Swiss banking — a business once synonymous with complete client confidentiality. “It was understood that when you said ‘Swiss banking,’ you meant absolute secrecy and absolute, inviolate trust,” he says.

Mr. Watts extends the argument to countries, like India, that have an enormous stake in the success of the BPO industry. They’d do much to allay fears by enhancing protection

sourcing providers] comply with the regulations.”

Countries like India that have an enormous stake in the success of the BPO industry would do much to allay fears by enhancing protection of intellectual property rights and enforcement of standards.

That said, there’s no reason to believe that offshoring necessarily entails greater risks. Professor Aron says that there is “absolutely no

in a CPI country. “There are few things an Indian or Chinese agent can do with a Social Security number,” says Professor Aron. “He cannot, from New Delhi or Shanghai, apply for a credit card.” He also notes that call center jobs are highly coveted in the CPI countries and employees are that much more worried about losing them, making them less likely to engage in delinquent behavior.

Jon Watts, on the other hand, suspects that incidents of violations are “highly underreported.” He worries that the industry won’t regulate itself until it’s forced to. “A major incident will trigger some reforms,” he says. “The vast weight of evidence says things like this don’t get addressed until something big happens. The ultimate challenge for the industry is to get ahead of this before something significant occurs.”

Countries like India that have an enormous stake in the success of the BPO industry would do much to allay fears by enhancing protection of intellectual property rights and enforcement of standards.

of intellectual property rights and enforcement of standards. Praful Mittal, an associate at Booz Allen in Chicago who has worked with financial-services and automotive companies on outsourcing such functions as human resources, IT, and overall product design and development, says that U.S. companies are concerned that India and the Philippines have no protections like the Sarbanes-Oxley Act of 2002. U.S. executives “want to make sure that when the CFO and the CEO sign off on the accounts, [the out-

data” to support the belief that offshore call centers are any more hazardous than U.S. call centers. “Most people I talk to seem to think that for every million transactions, there are more violations in the U.S. than in offshore call centers.” Professor Aron says that U.S. companies may actually expose themselves to fewer risks in offshore centers in the so-called CPI countries — China, the Philippines, and India — than back home. He argues that the incentive for misuse of credit card or Social Security information is much lower

strategy+business (www.strategy-business.com) and Knowledge@Wharton (<http://knowledge.wharton.upenn.edu>) publish white papers on contemporary global business issues, featuring the latest research and ideas from partners at Booz & Company and faculty from the University of Pennsylvania's Wharton School. *strategy+business* is a quarterly business thought-leadership magazine published by Booz Allen Hamilton. Knowledge@Wharton is an online resource for executives published biweekly by the Wharton School.