

powerchex
Specialising in supplier due diligence



Third Party Supplier Due Diligence

A necessary step to maintain business quality and safety

*Betrayal is the only truth that sticks –
Arthur Miller*

Companies rely on third party suppliers for their expertise in many seemingly harmless services: printing and mailing, off-site archiving of back up material, IT systems, cleaning, and security. The third party suppliers are expected to deliver these services to certain standards. They are depended upon not to falter after a contract is agreed, or to put the company and its clients at risk of crime.

When faced with a choice of third party suppliers, companies find themselves looking at potential partners who all appear to look good on paper. Apparently, they can meet the company's needs – and more. But how can the company be sure that these claims will be met? How can they know that entering into a contract with a given third party supplier will not, in fact, have adverse consequences they would prefer to avoid?

The purpose of this paper is to examine this problem. We will consider how it arises, what it may entail, and measures that companies can and should take to solve it.

Does that supplier really offer such a good service?

A third party supplier can easily hide that the service it offers is not of the quality it advertises. Over inflated claims on websites are rife, and are designed to snare companies into committing to contracts. Several third party suppliers vying for attention, all trying to out-do each other in today's ultra competitive market place, are always going to embellish and over emphasise what they offer.

In some cases, the suppliers have neither the equipment nor the expertise that they boast of. Staff may be incompetent and untrained, while

the directors, too, may be incompetent or have judgments against them. The existence of such defects, of course, would strongly suggest that a company will not be best served by that supplier. If aware of them prior to entering into a contract, a company would reasonably choose one of its better suited competitors.

Case Study 1: A fired director operates an accreditation agency

Maurice Dimmock was sacked from his post as director of international operations at Northumbria University. But he was approved to direct an accreditation agency for private colleges, The Accreditation Service for International Colleges (ASIC).

ASIC then approved a college which was a front for an immigration scam that smuggled over 1,000 illegal immigrants into the country. It approved another that sold bogus diplomas, netting £5 million for its owners, who later fled the country.

It was one of just seven such government approved organizations. It was run from a semi-detached house, and employed 5 staff including Mr Dimmock's 78 year old father.

"There is a lack of information and transparency about (ASIC's) management, governance and financial structures," said the chief executive of Universities UK.

Source: The Times, June 2009.

Measures that could have been taken to avoid this calamitous incident immediately emerge:

The government should have made sure that there was transparency about the governance and financial structures of ASIC. Only once they had an idea of how it works could the government be

sure that – as it had claimed – ASIC was capable of performing its job properly.

The government should also have investigated why the director had been removed from his previous post. It would have been highly advisable to compile a full report on his credentials and examined any discrepancies in detail. Only then could the government have had full confidence in approving ASIC as an accreditor.

Lest ye be judged!

A company's reputation is naturally correlated with the reputation of its third party suppliers. By associating, working and transacting with them, a company issues a statement that it approves of their practices.

But what happens if the associate of a company is found to operate unethical practices? What if it does a make-shift job? And what if all this went on beneath the nose of the company?

The company's reputation would be tarnished and stained. For example, if an overseas third party supplier admits of dishonest practices, or abuses the rights of its employees, the reputation of any company receiving its services would be damaged. Equally, a company's reputation would be damaged if one of its suppliers were defrauded. Its own customers could feel the effects, remove their custom and spread the word.

The reputational damage would be amplified if the company's clients or the media discovered that the company had failed to take necessary precautions. The fact that company failed to investigate the reputation and quality of practices of a third party supplier would discredit it. Indeed, an excellent example of this is the criticism and negative media attention the government faced for its failings in case 1.

To avoid this possibility, a company would need to contact numerous clients of the supplier for references on how it has performed in the past. In addition, it should check for any negative media reports on the supplier. These two measures, however, are not a fail-safe. Companies are sometimes referred to third party suppliers by people they know, and put themselves at risk by neglecting to make the aforementioned checks into quality and reputation.

Case Study 2: Insurance claims handler hires contractors from Yell.com

Aspray Limited failed to control its business network by not "maintaining appropriate systems and controls for the recruitment, training and monitoring" of its appointed representatives.

In some cases, it had failed to make financial checks, compliance visits, and review the files of its appointed representatives.

It is a franchise company that manages insurance claims for property repairs. The FSA fined Aspray for failing to control its business network.

Source: FSA, March 2009

This company could have done more to ensure that its appointed representatives were bona fide and performing to the expected level. This posed a risk to their customers and their reputation. And they paid a price in the form of a fine of tens of thousands of pounds.

It would have been far more economical for the company to invest in checking the equipment and capabilities of their contractors. This could be achieved through an on-site audit and an interview enquiring about their policies concerning governance, security, and whether they hold necessary industry affiliations and qualifications.

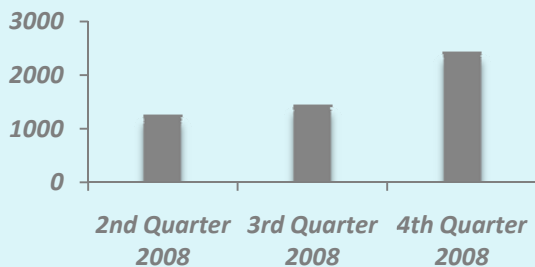
Reliability in the Recession

One of the most difficult global economic climates witnessed for years poses two main problems for companies regarding their third party suppliers. Can they be trusted not to join the overflowing graveyards of collapsed businesses? And will they invest enough resources in guarding the company's sensitive information?

Sinking Suppliers?

Unthinkingly, companies may enter into a contract with a supplier without ensuring that the supplier is capable of providing their service reliably, and for a sustained amount of time. Companies rely on their third party suppliers for essential services. It is simply not good enough if a supplier has to make changes to the quality of the service they provide soon after entering into a contract; it is even worse if a supplier is forced into administration shortly after it strikes up a business relationship with a company. The company's own functioning would be impaired – possibly to the extent that it may itself fail to see to the needs of its own clients. The company would additionally have to invest money and time in selecting a replacement.

Fig.1: Spiralling Corporate Insolvencies



The level for the fourth quarter of 2008 is a 220% rise from that of the previous year.

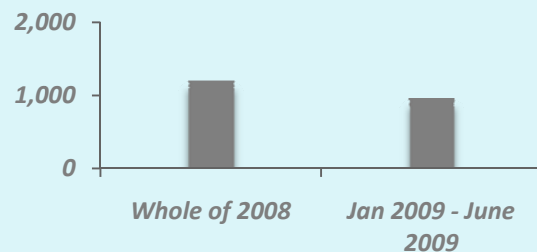
Source: The Insolvency Service

Companies can protect themselves from a supplier failing prematurely. They should ensure that they know the supplier's credit history, and have seen up-to-date financial statements stretching back at least a couple of years. Thus, a company can know that the third party supplier is currently financially robust and has a history of being so. Background checks into the supplier's directors' history would certainly be helpful for this purpose.

Secure Suppliers?

Companies often enter into contracts with third party suppliers without knowing the strength of the suppliers' security measures. Yet suppliers are trusted with access to sensitive data of the company and its customers. This introduces a number of security risks to the company itself – risks which are amplified by the current economic climate.

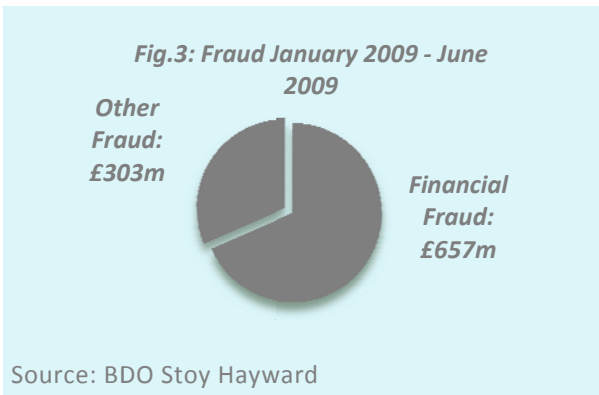
Fig. 2: Escalating Fraud (£ millions)



Source: BDO Stoy Hayward

By giving third party suppliers access to its sensitive information, a company can expose itself and its customers to the risk of fraud. The scale of the risk is highlighted in figure 2, which shows that fraud levels have almost doubled since a year ago; fraud experts at the accountancy firm BDO Stoy Hayward predict that they may more than double by the end of 2009, reaching £3 billion before the end of the recession. The scale of the risk specifically for the financial sector is depicted by figure 3, below. It is a widespread and fast

growing threat. It is increasing so quickly partly because businesses are reducing their security budgets as the recession bites.



When a company allows a third party supplier access to the personal data of its customers, the legal responsibility for the data remains with the company (in accordance with the Data Protection Act, 1998). Companies are legally required to ensure that third parties are capable, reliable and have sufficient controls in place to maintain the confidentiality and safety of their customers' data. But research has shown that companies often rely primarily on clauses in contracts with third party suppliers to guarantee the safety of their customers' (and their own) data. The FSA's *Data Security in the Financial Services 2008* report found the following examples of bad practice:

- Companies not knowing exactly which third party staff have access to their customer data.
- A lack of awareness of when/how third party suppliers can access customer data and failure to monitor such access.
- Allowing third-party suppliers to access customer data when no diligence of data security arrangements has been performed.

The ramifications of data loss can be very significant. As the figures 2 and 3 show, it costs the financial sector a large amount of money – even more than we can know about, since fraud can go undetected. Data loss can also lead to distress and inconvenience for a customer whose identity is stolen. And the proceeds from identity theft are known to underpin other forms of organized crime, such as the trafficking of drugs and people, as stolen details are used to forge travel documents.

Case Study 3: Fraudster's request over £1.5m from financial administrator

Within the timescale of two months, £1.5m was requested from over 20 clients of Capita Financial Administrators (CFA). Fraudsters received £328,241 in actual payments.

The FSA fined CFA, a third party administrator that carries out client instructions to buy and sell investments, £300,000 for failing to have robust anti-fraud controls.

Source: FSA, March 2006

Companies can combat the risk of data loss through a third party supplier with several preventative precautions. They should ensure that suppliers' IT systems meet standards recommended by governing bodies and the information commissioner. They must check suppliers' governance policies regarding data security: they should find out that there is a data security manager, that staff are trained to be secure with sensitive data, and that there is a written policy which meets the minimum standards to guarantee that sensitive information for which the company is responsible remains safe. Overall, the company can protect their data by avoiding the bad practice listed to the left. This could be established through a visit to the company, or an

interview over the phone, as would be expected when an important business deal is about to be agreed.

*Don't let me down, don't let me down,
please – The Beatles*

It clearly is in a company's best interest to make sure that its suppliers are the best it could have. But companies are failing to take the necessary steps to make this happen. They risk subjecting themselves and their clients to a variety of negative impacts by striking up deals with suppliers who may be sub-standard, on the verge of going into administration, or careless with their data.

Throughout the paper we have suggested several ways manage this risk. We have further developed a screening service that encompasses these means into a cohesive and flexible package for all types of companies. Please ask for details.

Powerchex Limited

Gun Court, 70 Wapping Lane, London E1W 2RD

Tel: 0870 710 3000 / 0207 767 2425, Fax: 0207 709 0706 / 0870 710 3000

Website: www.powerchex.co.uk

Managing Director: Alexandra Kelly akelly@powerchex.co.uk

Author: Deva Gilroy Sen