HOW DOES INFORMATION SECURITY IMPACT YOU?

TrustedImpact
PROTECTING DIGITAL

TrustedImpact Pty Ltd, Level 9, 22 Albert Road, South Melbourne 3205
secure@trustedimpact.com, (03) 9023-9710

Have you outsourced your reputation to someone who doesn't care?

The growth of outsourcing and partnering (both in Information Technology and other non-core business processes) has been impressive. Aggressive and innovative companies have implemented a range of outsourced operations under the 'battle cry' of significant cost savings, improved economies of scale, and improved ability to focus on their core business, among others.

Indeed there are many opportunities to achieve significant business benefits from outsourcing. But if the structure of the opportunity does not reflect the importance of sensitive information that may be outsourced, the company risks placing its brand and reputation in the hands of a third party who frankly has no incentive (direct or indirect) to protect this information from inappropriate use.

In fact, empirical evidence from a study of over 500 recent breaches of sensitive data found that 13% of all data breaches were a result of a third party. Whilst the initial company may have legal alternatives to recover the cost associated with responding to this lost sensitive data, at the end of the day, the consumer has trusted the original company to protect their information.

Ultimately the outsourcers are usually not motivated to protect their clients' data – in fact, it's generally the opposite. Typically, specific contractual performance-based Service Level Agreements (SLA's) are defined around keeping operations running smoothly. Their key focus is generally on throughput, efficiencies, availability and cost, depending on the type of arrangement. The outsource vendors are then incentivised to achieve a difficult balance between a) achieving the contractual SLA's, at b) the absolute minimum of cost. Those outsourcer Account Managers who can maintain the SLA's at lower cost are recognised as the top performers who receive their bonuses and recognition. If the protection of your sensitive information is not a well defined and focused "SLA", you can be guaranteed there is little concern about its protection.

Objectives of outsourcing

The IT outsourcing movement began in the 1990's primarily as a means of reducing and controlling the spiralling costs of operations. Typically the function of a fixed task, such as a help-desk call centre was divested on to another organisation to be performed under specific guidelines.

Other intended benefits of the approach were to access the outsourcer's specialised skill-sets and best practice methodologies, while freeing up key internal personnel from doing the basic operational tasks to allow them to focus on performing projects towards the growth of the business.

Unfortunately experience has shown that these additional benefits were often negated, with the outsourcer hiring or contracting the existing key internal personnel, which then left business development projects running with extensive management and the remainder non-key personnel. This is demonstrated by the high failure rates of projects at the time.

Evolution to Business Process outsourcing

The IT department's direct and contract employees have traditionally been the front-line caretakers of the business's information, and have provided the baseload of service operation tasks. Due to a desire to reduce capital expenditures in favour of operating budgets, recently critical core business processes are also being outsourced, such as IT Security, R&D and tasks involving direct customer contact.

The continuation and extrapolation of the Process outsourcing model could see organisations divesting all but the fundamental core focus in which they choose to specialise.

In 2007 the worldwide market for outsourcing was estimated to be US$235bn[1] (per figure 1). With the current trend of outsourcer's providing more and more core business process functions, even the most conservative predictions estimate double digit growth over the next five years.

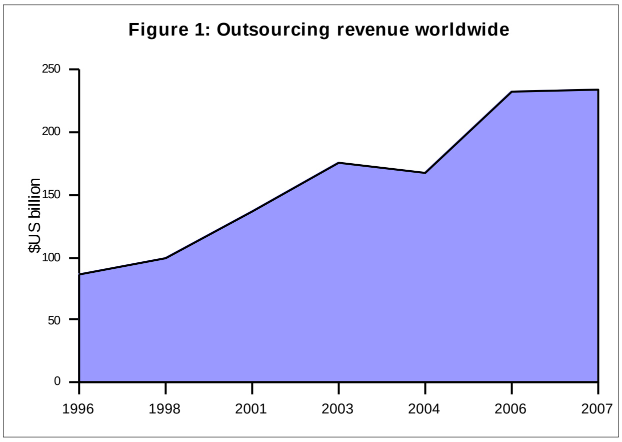
Figure 1: Outsourcing revenue worldwide

Objectives Increased Risks of Process Outsourcing

Where previously outsourced tasks could be securely accomplished within the confines of the 'least privilege' principle of minimum access requirements, advanced tasks such as database management and network analysis required outsourcer's to be provided with comprehensive access to the entirety of operational data.

Even just evaluating the outsourcing concept in itself can open system integrity issues, such as sabotage or data theft from a disgruntled employee. The transition of a task to outsourcing needs to be carefully assessed and monitored within the context of the organisations Business Continuity Plan.

Advanced Business Process outsourcing has exponentially increased the potential for a data breach, causing headaches for IT Security staff and liability issues for Company Directors[2]. The data leakage of customers private records, credit card information, internal emails, and Intellectual Property has decimated businesses virtually (and literally) overnight. A general 'ballpark' estimate figure for the cost of a breach is US$182 per customer record [3] .

Offshoring: high risk – high return

A subset of outsourcer's leverage additional cost savings by utilising resources from other countries where they may access a cheaper labour market. This has become a viable alternative in recent years due to the improving availability and integrity of global communications infrastructure. A call centre can be relocated anywhere in the world via a simple phone redirection and network connectivity via an encrypted link. To minimise end-user impacts, offshorers train their phone operators with localised accents and colloquial slang to provide a familiar persona, and staff are even updated on their customers' local sporting results in order to recreate a friendly repertoire.

A basic Microsoft MCSE System Administrator contracts for around $40-$60 per hour[4] in Australia, compared to less than $6 per hour in India[5]. This dramatic cost saving is tethered by management challenges in ensuring the integrity of the process in a diverse and sometimes volatile political, cultural and regulatory structure.

For example, the Corruption Perception Index (CPI) 2006 [6] lists Australia in 9th position, with common offshore locations India and China both in equal 70th place. A thorough Risk Analysis is required to determine the placing

[1] Figure 1 data is a composite of IDC (1996-2001), Gartner (2003/07), Datamonitor (2004), & Frost & Sullivan (2006).

[2] Crampton, Trusted**Impact**; Emerging obligations and personal liability of Directors

[3] 2006 Survey; The Cost of Data Breach – Ponemon Institute

[4] From a random sampling via http://www.seek.com.au

[5] From a random sampling of sites such as http://www.supportresort.com

[6] http://www.transparency.org/policy_research/surveys_indices/cpi/2006

of suitable controls relative to conditions in offshore environments.

Who has your customer data?
Where is your customer data?
What are the existing controls?
Are they adequate and appropriate?

Future Trends: Multisourcing

Rather than relying on single large-scale outsourcing partners to provide external services, businesses are now evolving to a distributed 'Multisourcing' model, where key functions are provided by specialist organisations as part of a multi-group service chain.

This avoids dependence on a single outsource vendor relationship, but once again further complicates the management of delivering the overall end-to-end service.

Balancing Objectives

The quality of service provided by an outsourcer is measured against key Service Level Agreements (SLA's), with often the focus and clear definition of these measures being the first step to a successful venture. This is an attempt to categorise and measure performance in order to maintain and review the standard of service provided over time.

Common trends have shown however, after the initial engagement the outsourcer company stakeholders inevitably seek increasing yearly returns from the deal. This triggers a precarious streamlining of the service operation so as to be focused only around reaching the minimum required SLA objectives.

Regardless of the good faith applied in defining the outsourcing contract, changes over the term of the engagement often require reassessment. It is not in the best interest of the client business if market forces have caused the venture to become unprofitable for the outsource organisation. In practice, a reliant symbiotic partnership is only successful if each component is also individually successful.

Defining Focus

Although they are required to fulfil the tasks as defined, outsourcers are not usually a motivated stakeholder in representing the end-user organisation. If performance bonuses or incentive options are applied, these need to be carefully defined to avoid further enticing the outsourcer to focus on that single objective.

It is recommended to engage a third party to assist in the development or renewal of an outsourcing contract. An independent party assists in the objective definition of a comprehensive SLA framework, as well as incorporating the outsourcer's strict adherence to the client's businesses governing IT policy.

Ongoing, a regular security assessment is essential to ensure the outsourcer's service baseline of SLA compliance. Preferably however, further assessment is recommended via an overall Security Assessment 'Check-up', as to whether the 'in principle' provision of services is satisfactory or whether further SLA's need to be defined. For extensive or high visibility outsourced tasks, an additional Gap Analysis may be performed to ensure correlation of business policies, culture and customer impact.

Ongoing, a regular security assessment is essential to ensure the outsourcer's service baseline of SLA compliance.

Getting on the same page...

To structure a more seamless framework by which outsourcer's are engaged, it is recommended to incorporate the adherence to the overall businesses strategy within the contract, rather than simply relying on a schedule of SLA compliance.

Due to the increasing technical and logistic requirements in recent years most organisations have sought to consolidate their strategic approach by implementing a governing IT Policy to standardise practice and procedures. Several international organisations have developed guideline templates towards defining a common best practice operational and regulatory methodology.

Further to this, businesses began offering proprietary frameworks with associated membership, accreditation and audit fees. In addition to voluntary policy considerations, an abundance of regulatory controls have also been imposed. This has now led to an array of IT governance standards / frameworks / protocols / guidelines.

Aligned for Security and Success

By adjusting from an SLA focused contract to IT Policy compliance framework allows for a more results driven approach. This also provides the outsourcer incentive for organic development and growth. New technologies or new features in updated version releases are then actively evaluated and considered within the context of the business overall security policy, and proposed in the interest of all stakeholders.

Overall, businesses are demanding outsourcer's be more and more synchronised with their general internal corporate policies and culture, such as requiring compliance with environmental 'green policies' [7]. This alignment ensures that the full life-cycle of the businesses information is protected. For example, the correct disposal of old retired PC's hard drives and data storage equipment has been highlighted by several instances of data breach [8].

TrustedImpact

We are uniquely positioned in the market to assist all organisations to unlock value and become more effective in managing information and its delivery technologies.

Trusted**Impact** is an independent information security and risk consultancy. We bear no allegiance with any vendor, partner or other organisation.

Australian-owned, invested and focused - we are committed to the ongoing success of Australian enterprises and have a deep understanding of the relevant issues in the local environment.

Our approach is to uniquely combine solid business knowledge and experience with a deep technical understanding and expertise in information security and risk management to define pragmatic, reliable solutions to improve your business. We are people driven to help other people succeed. It’s not just about technology; it's about helping your people become more effective.

Author

Steve Judd is a 15 year veteran of the IT industry, including over 10 years from an Information Security based perspective. Working with Trend Micro, Computer Associates, and Fujitsu, as well as 7 years as a contractor and consultant, he has experience with most of the Enterprise businesses in the country. Steve was one of the first Certified Information Systems Security Professionals (CISSP) in Australia, on several occasions has been asked to write advisory submissions on IT policy for the Senate, and maintains a very broad and detailed knowledge on all aspects of IT and its business application. He holds a Defence Security Clearance, along with a host of other certifications and qualifications.

Steve is a Principal Consultant at Trusted**Impact**, and may be contacted via phone on (03) 9023 9710 or email via steve.judd@trustedimpact.com

[7] Brown-Wilson, The Black Book of outsourcing

[8] http://www.pcworld.com/article/125662-1/article.html, http://www.simson.net/clips/2003/2003.CSO.04.Hard_disk_risk.htm, http://www.theregister.co.uk/2005/04/07/hard_drive_with_police_info_sold_on_ebay/